



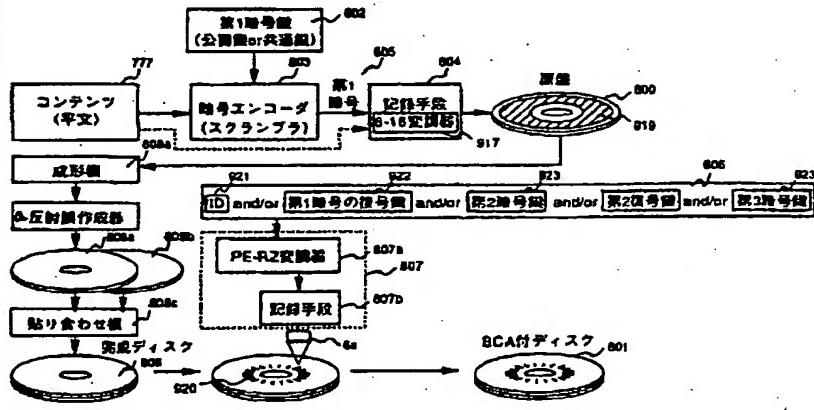
PCT

世界知的所有権機関  
国際事務局  
特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 7/00, 20/10, G06F 12/14, 9/06	A1	(11) 国際公開番号 <b>WO97/14144</b>
		(43) 国際公開日 1997年4月17日(17.04.97)
(21) 国際出願番号 PCT/JP96/02924		
(22) 国際出願日 1996年10月8日(08.10.96)		
(30) 優先権データ 特願平7/261247 特願平8/8910 特願平8/211304	1995年10月9日(09.10.95) 1996年1月23日(23.01.96) 1996年8月9日(09.08.96)	JP JP JP
(71) 出願人(米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP] 〒571 大阪府門真市大字門真1006番地 Osaka, (JP)		小石健二(KOISHI, Kenji)[JP/JP] 〒669-13 兵庫県三田市けやき台3-56-8 Hyogo, (JP) 守屋充郎(MORIYA, Mitsuru)[JP/JP] 〒630-01 奈良県生駒市ひかりが丘3丁目1番29号 Nara, (JP) 竹村佳也(TAKEMURA, Yoshinari)[JP/JP] 〒566 大阪府茨木市別府2-8-11 Osaka, (JP)
(72) 発明者: および (75) 発明者/出願人(米国についてのみ) 大嶋光昭(OSHIMA, Mitsuaki)[JP/JP] 〒615 京都府京都市西京区桂南町115-3 Kyoto, (JP) 後藤芳穂(GOTOH, Yoshiho)[JP/JP] 〒536 大阪府大阪市城東区東中浜4-9-17-201 Osaka, (JP) 田中伸一(TANAKA, Shinichi)[JP/JP] 〒610-03 京都府綾喜郡田辺町山手東1-42-14 Kyoto, (JP)		(74) 代理人 弁理士 滝本智之, 外(TAKIMOTO, Tomoyuki et al.) 〒571 大阪府門真市大字門真1006番地 松下電器産業株式会社内 Osaka, (JP)
		(81) 指定国 CN, JP, KR, US, 欧州特許(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
		添付公開書類 国際調査報告書

(54) Title: OPTICAL DISK, OPTICAL RECORDER, OPTICAL REPRODUCING DEVICE, ENCRYPTED COMMUNICATION SYSTEM, AND AUTHORIZING SYSTEM FOR USE OF PROGRAM

(54) 発明の名称 光ディスクおよび光記録装置および光再生装置および暗号通信方式およびプログラム使用許可方式



a ... reflecting film forming device  
 777 ... contents (ordinary writings)  
 800 ... raw disk  
 801 ... disk with BCA  
 802 ... first ciphering key (public or common key)  
 803 ... cipher encoder (scrambler)  
 804, 807b ... recording means  
 805 ... first cipher  
 806 ... second decoding key  
 807a ... PE-RZ modulator  
 808a ... molding machine  
 808c ... sticking machine  
 809 ... finished disk  
 917 ... B-16 modulator  
 922 ... first cipher decoding key  
 923 ... second ciphering key  
 923a ... third ciphering key

## (57) Abstract

Various kinds of procedures including the operating procedure of a network-based disk application system are simplified. An auxiliary information recording area is provided on the optical disk to store a different IDs, encryption keys and decryption keys on different disks at the factory. The number of procedures required on the user side can be reduced by using IDs to decrypt software, encryption keys to send cryptograms, and decryption keys to receive cryptograms.

## (57) 要約

ネットワーク利用型の光ディスクの応用システムの操作手順や諸手続きを簡便化する。

光ディスクに副情報記録領域を設け、ディスク毎に異なる ID や暗号鍵や復号鍵

を工場で記録しておく。使用者がソフトの暗号解除には ID、暗号送信時に暗号鍵、暗

号受信時に復号鍵を用いることにより手順や手続きを省略できる。

## 情報としての用途のみ

PCTに基づいて公開される国際出願をパンフレット第一頁にPCT加盟国を同定するために使用されるコード

AL アルバニア	EE エストニア	LS リベリア	RU ロシア連邦
AM アルメニア	ES スペイン	LT リトアニア	SD スーダン
AT オーストリア	FIR フィンランド	LU ルクセンブルグ	SG スウェーデン
AU オーストラリア	FR フランス	LV ラトヴィア	SGG シンガポール
AZ アゼルバイジャン	GAB ガボン	MC モナコ	S1 スロヴェニア共和国
BB ベルバドス	GBB イギリス	MD モルドバ	SKN スロヴァキア共和国
BE ベルギー	GE グルジア	MG マダガスカル	SZD セネガル
BF ブルガニア・ファソ	GH ガーナ	MK マケドニア旧ユーゴスラ	SZG スウェーデン
BG ブルガリア	GN ギニア	WIA 共和国	TG チャード
BJ ベナン	GR ギリシャ	ML マリ	TJ トジキスタン
BR ブラジル	HU ハンガリー	MN モンゴル	TM トルクメニスタン
BY ベラルーシ	IIE アイルランド	MR モーリタニア	TR トリニダード・トバゴ
CA カナダ	IST アイスランド	MW マラウイ	TT トライニティ・タバコ
CF 中央アフリカ共和国	ITP イタリア	MX メキシコ	UAG ウクライナ
CG コンゴ	KE ケニア	NEL ニジェール	UGS ウガンダ
CH スイス	KGP キルギスタン	NO オランダ	UZ ベキスタン共和国
CI コート・ジボアール	KP 朝鮮民主主義人民共和国	NOLO ノルウェー	VZN ヴィエトナム
CM カメルーン	KR 大韓民国	PLT ニュージーランド	YU ユーゴスラビア
CN 中国	KZ カザフスタン	PPT ポルトガル	
DE チェコ共和国	LK リヒテンシュタイン	RO ルーマニア	
DK ドイツ			
DK デンマーク	LK スリランカ		

WO 97/14144

PCT/JP96/02924

## 1

## 明細書

## 発明の名称

光ディスクおよび光記録装置および光再生装置および暗号通信方式およびプログラム

## 5 使用許可方式

## 技術分野

本発明は光ディスクおよび光ディスクシステムおよび暗号通信方法に関するものである。

10

## 背景技術

近年、インターネット等のネットワークと光ROMディスクの普及に伴い、光ROMディスクを用いたネットワークソフト流通が始まりつつある。また電子商取引きの検討が進んでいる。

15 従来技術として、CD-ROMをメディアとして用いたソフト電子流通システムが実用化されている。この場合パスワードを与えて、CD-ROMに予め記録された暗号化されたソフトの暗号を解くといった方法が一般的である。しかし、CD-ROMの場合、ディスク上に追記記録できないため各ディスクのIDは個別に設定できない。従って単純に用いれば、1つのパスワードが同一原盤から製造された全てのディスクの暗号を解  
20 除してしまう。このため、CD-ROMを用いた場合、各々のディスク個有のIDをパソコン側のハードディスク上に作成したり、センターで作成したIDを郵便によりユーザーに送るという作業が必要であった。

従来の光ディスクや光ディスクシステムを用いた電子流通システムにおいては、光ディスクもしくはシステムにIDや暗号鍵を簡便に供給することが求められている。本發

WO 97/14144

PCT/JP96/02924

## 2

明はROMディスクを用いた電子流通システムにIDと暗号鍵の簡便な供給を実現することを目的とする。

## 発明の開示

- 5 この課題を解決するために、光ディスクのピット部にバーコードを重ね書きした追記領域（以下BCAと略す）を設け光ディスク製造時に、BCA領域にディスク毎に異なるIDと必要に応じて通信用の暗号鍵、通信用の復号鍵暗号文の復号鍵を個別に記録しておくことにより、ディスクをユーザーに配布した時点で、ユーザーにはユーザーID番号と通信用の送信用の暗号鍵、受信用の復号鍵の3つが自動的に配布されていること  
 10 になり、従来のシステムを複雑にしていたいくつかの手順が省略できる。こうして、暗号通信とコンテンツの入ったディスクの識別が同時に実現する。

## 図面の簡単な説明

- 第1図は本発明の実施例の光ディスクの工程図、第2図は本発明の実施例のパルスレーバーによるトリミングの断面図、第3図は本発明の実施例のトリミング部の信号再生波形図、第4図は本発明の実施例の再生装置のブロック図、第5図（a）は本発明のBCA部の再生信号波形図、第5図（b）は本発明のBCA部の寸法関係図である。

- 第6図は本発明の実施例の暗号通信の方法とパスワードによる暗号鍵の方法、第7図は本発明のBCAのフォーマット図、第8図は本発明の実施例の暗号通信の方法とパスワードによる暗号解鍵の方法、第9図は本発明の実施例のコンテンツ部分を使用許可したディスクの動作手順図である。

- 第10図は本発明の実施例のRAMディスクにBCAを記録した場合のブロック図、第11図は本発明の実施例の不正コピー防止方式のブロック図、第12図は本発明の実施例の不正コピー防止のフローチャート図、第13図は本発明の実施例のBCAに商品

WO 97/14144

PCT/JP96/02924

バーコードを印刷した光ディスクの上面図と断面図、第14図は本発明の実施例のB C A付ROMディスクとPOS端末を用いたPOS決済システムのブロック図である。

第15図は本発明の実施例のプレス工場とソフト会社と販売店の暗号解除の流れ図、第16図は本発明の実施例のディスクID等を用いた暗号データの暗号化複合化ステップのフローチャート図（その1）、第17図は本発明の実施例のディスクID等を用いた暗号データの暗号化複合化ステップのフローチャート図（その2）、第18図は本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート図（その1）、第19図は本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート図（その2）、第20図は本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート図（その3）である。

第21図は本発明の実施例のBCAを用いた電子決済システムのフローチャート図（その1）、第22図は本発明の実施例のBCAを用いた電子決済システムのフローチャート図（その2）、第23図は本発明の実施例のBCAを用いた電子決済システムのフローチャート図（その3）、第24図は本発明の実施例のBCAを用いた1枚のRAMディスクに記録制限する記録再生方法のブロック図である。

#### 発明を実施するための最良の形態

実施例に基づき、本発明を説明する。なお、本文ではBCA方式を用いた追記領域をBCA領域、BCAにより記録されたデータをBCAデータと呼ぶ。また第1識別情報はID、もしくはディスクIDとも呼ぶ。

第1図はBCA付デスクの代表的な工程を示す。まず、公開鍵等の第1暗号鍵802を用いて暗号エンコーダ803でコンテンツ777が暗号化された第1暗号805がマスキング装置等の8-16変調器917により変調され、この変調信号がレーザーにより原盤800の第1記録領域919に凹凸のピットとして記録される。この原盤80

訂正された用紙（規則91）

WO 97/14144

PCT/JP96/02924

## 4

0を用いて成形機808aでディスク状の透明基板918を成形し、反射膜作成機808bでA1反射膜を形成し0.6ミリ厚の片面ディスク809a、809bを作成し、貼り合わせ機808cで貼り合わせた完成ディスク809の第2記録領域920にトリミング装置807で、ディスクID921もしくは第1暗号の復号鍵922もしくはインターネット通信用の第2暗号鍵923をPE変調とRZ変調を組み合わせたPE-RZ変調器807aで変調し、パルスレーザー807bでBCAトリミングして、BCA付きディスク801を製造する。貼り合わせディスクを用いているので、中に入ったBCAは改ざん出来ず、セキュリティ用途に用いることが出来る。

説明に入る前に、BCAについて、簡単に説明する。

第2図の(1)に示すようにBCAでは2層ディスク800にパルスレーザー808で、アルミ反射膜809をトリミングし、ストライプ状の低反射部810をPE変調信号に基づいて記録する。第2図(2)に示すようにBCAのストライプがディスク上に形成され、このストライプを通常の光ヘッドで再生するとBCA部は反射信号がなくなるため第2図(3)に示すように変調信号が間欠的に欠落した欠落部810a、810b、810cが発生する。変調信号は第1スライスレベル915でスライスされる。一方欠落部810a等は信号レベルが低いので、第2スライスレベル916で容易にスライスできる。図3の記録再生波形図に示す様に、形成されたバーコード923a、923bは、第3図(5)に示すように通常の光ピックで第2スライスレベル916でレベルスライスすることにより再生可能で第3図(6)に示すようにLPFフィルタで波形成形されPE-RZ復調され、(7)に示すようにデジタル信号が出力される。図4を用いて復調動作を説明する。まず、BCA付のディスク801は透明基板が2枚、記録層801aが中にくるように貼り合わせてあり、記録層801aが1層の場合と記録層801a、801bの2層の場合がある。2層の場合は光ヘッド6に近い第1層の記録層801aのコントロールデータにBCAが記録されているかどうかを示すBCAフラ

WO 97/14144

PCT/JP96/02924

## 5

グ922が記録されている。BCAは第2層801bに記録されているので、まず第1層記録層801aに焦点を合わせ第2記録領域919の最内周にあるコントロールデータ924の半径位置へ光ヘッド6を移動させる。コントロールデータは主情報なのでEFM又は8-15又は8-16変調されている。このコントロールデータの中のBCAフラグ922が‘1’の時のみ、1層、2層部切換部827で、焦点を第2記録層801bに合わせてBCAを再生する。レベルスライサー590で第2図(3)に示すような、一般的な第1スライスレベル915でスライスするとデジタル信号に変換される。この信号を第1復調部においてEFM925又は8-15変調926又は8-16変調92の復調器で復調し、ECCデコーダ36でエラー訂正し主情報が出力される。この10 主情報の中のコントロールデータを再生し、BCAフラグ922が1の場合のみBCAを読みにいく。BCAフラグ922が1の時、CPU923は1層、2層部切換部827に指示を出し、焦点調節部828を駆動して、第1層の記録層801aから第2層の記録層801bへ焦点を切り替える。同時に第2記録領域の920の半径位置、すなわちDVD規格の場合はコントロールデータの内周側の22.3mmから23.5mmの間に記録しているBCAを光ヘッド6を移動させ、BCAをよみとる。BCA領域では第2図(3)に示すようなエンベロープが部分的に欠落した信号が再生される。第2レベルスライサ929において第1スライスレベル915より低い光量の第2スライスレベル916を設定することにより、BCAの反射部欠落部は検出でき、デジタル信号が<sup>15</sup>出力される。この信号を第2復調部930においてPE-RZ復調し、ECCデコーダ930dにおいてECCデコードすることにより副情報であるBCAデータが出力される。このようにして、8-16変調の第1復調器928で主情報をPE-RZ変調の第2復調部930で副情報つまりBCAデータを復調再生する。

第5図(a)にフィルタ943通過前部の再生波形、(b)に低反射部810のスリットの加工寸法精度を示す。スリットの巾は5~15μm以下にすることは難しい。ま

WO 97/14144

PCT/JP96/02924

## 6

た、23.5 mmより内周に記録しないと記録データを破壊してしまう。このことからDVDの場合最短の記録周期=30 μm、最大半径=23.5 mmの制限からフォーマット後の最大容量は188 bytes以下に限定される。

変調信号は、8-16変調方式を用いてピットで記録されており、第5図(a)の高周波信号部933のような高周波信号が得られる。一方、BCA信号は低周波信号部932のような低周波信号となる。このように、主情報がDVD規格の場合、最高約4.5 MHzの高周波信号932であり、第5図(a)に示すように、副情報が周期8.92 μsつまり約100 KHzの低周波信号933であるため、LPF943を用いて副情報を周波数分離することが容易である。第4図に示すようなLPF943を含む周波数分離手段934で、2つの信号を容易に分離することが出来る。この場合、LPF943は簡単な構成でよいという効果がある。

以上がBCAの概略である。

では、第6図を用いて、暗号ソフト解錠システムの全体システムをパスワード発行と暗号通信と発注者の認証の動作に絞り説明する。まず、プレス工場のステップは、第1図の場合とほぼ同じ手順で製造されるので、原盤800と完成ディスク809の図は省略する。

プレス工場811において、第1~n番目のコンテンツの平文810は暗号エンコーダ812により、各々第1~n番目の暗号鍵813でデータの暗号化又は映像信号のスクランブルがなされ、光ディスクの原盤800に記録される。この原盤800から、プレスされて製造されたディスク状の基板809に反射膜が形成された後に、2枚のディスク状の基板を貼り合わせた後、完成ディスク809が作られる。この完成ディスク809に、ディスク毎に異なるID815もしくは/かつ第1暗号鍵816(公開鍵)もしくは/かつ、第2暗号鍵817(公開鍵)、第2コンピュータの接続アドレス818がBCA領域814に記録されたBCA付ディスク801が、ユーザーに配布される。

WO 97/14144

PCT/JP96/02924

このディスクのコンテンツは暗号化されているので、再生するには代金等の代価を払って  
パスワード発行センターつまり電子商店もしくは、モールからパスワードをもらう  
必要がある。この手順を述べる。

- ユーザーの第1コンピュータ809では配布されたBCA付きディスク801を再生  
5 装置819で再生すると、PE-RZ復調部を含むBCA再生部820により、ID8  
15、第1暗号鍵816、第2暗号鍵817、接続アドレス818のデータが再生され  
る。パスワードをもらうためには、パスワード発行センター821のサーバーである第  
2コンピュータ821aの接続アドレス818へ通信部822を介してインターネット  
等のネットワーク823経由で接続し第2コンピュータ821aへIDを送信する。  
10 ここで、暗号通信の手順について述べる。第2コンピュータ821aはユーザーの再  
生装置819からのID815を受信する。すると“モール”や“電子商店”とよばれ  
るパスワード発行センター821の第2コンピュータすなわちサーバー821aは暗号  
鍵データベースDB824をもつ。このデータベースにはこのディスク個有のIDもし  
くはIDの第1暗号鍵816に対応する復号鍵である秘密鍵、つまり第1復号鍵825  
15 とIDの表が収容されている。従ってサーバーは受信したIDをもとに第1復号鍵82  
5を検索することができる。こうして第1コンピュータから第2コンピュータ821a  
への暗号通信が成立する。この場合、第1暗号鍵と第1復号鍵は公開鍵暗号ではなく、  
共通鍵暗号の共通鍵ならば同じ鍵となる。  
20 利用者はディスク801の中に、例えば、1000本収納されている暗号化されたコ  
ンテンツの1部、例えばコンテンツ番号826がnのコンテンツを利用したい場合、コ  
ンテンツ番号826つまりnを第1暗号鍵816である公開鍵を用いて、公開鍵暗号関  
数から構成される第1暗号エンコーダ827で、暗号化した暗号を第2コンピュータ8  
21aに送信する。第2コンピュータ821a側では前述のようにこの暗号を復号する  
ための第1復号鍵825を検索し知っている。従ってこの暗号を確実に平文化できる。

こうしてユーザーの発注情報のプライバシーは暗号により守られるという効果がある。

この場合第1暗号鍵816として公開鍵暗号の秘密鍵を用いて署名してもよい。この方法は“デジタル署名”と呼ばれる。詳しい動作の説明は、暗号の専門書例えば、“E-Mail Security by Bruce Schneier 1995”の5 “Digital Signature”の項目等を参照されたい。

暗号通信にもどるとこの暗号は通信部822とネットワーク823を介して、パスワード発行センター821の第1暗号デコーダ827に送られる。こうして、第1暗号鍵816と対になっている第1対暗号鍵825を用いて第1対暗号デコーダ827では、暗号が復号される。

10 この場合、公開鍵は特定の1枚のディスクしかもっていないため、第3者のディスクからの不正な注文は排除できる。つまり、1枚のディスクの認証ができるためこのディスクの持ち主のユーザー個人の認証ができる。こうしてこのコンテンツ番号nは特定の個人の注文であることが証明されるため、第3者の不正な注文は排除できる。

15 この時公開鍵816を秘密にしておけば、この手法でクレジットカード番号等の高いセキュリティが要求される課金情報の送信にも技術的には用いることができる。しかし、通常“モール”と呼ばれる店では、セキュリティの保証がないため、電子決済ではユーザーの課金情報は扱わない。クレジットカード系と銀行系の課金センター828のみが、ユーザーの金融情報を取り扱うことができる。現在、SET等のセキュリティ規格の統一化が進められており、RSA1024bitの公開鍵暗号が使われ金融情報の暗号化が実現する可能性が高い。

次に本発明の場合の課金情報の暗号通信手順を示す。まず、BCA再生部820で再生された公開鍵暗号の第2暗号鍵817を用いて、個人のクレジットカード番号等の課金情報830は第2暗号エンコーダ831により、RSA等の公開鍵系暗号により、暗号化され、通信部822より第2コンピュータ821を介して第3コンピュータ828

の暗号デコーダ832に送られる。この場合デジタル署名をする場合は第2暗号鍵817は秘密鍵829を用いる。

5 パスワード発行センター821の第2コンピュータ821aの暗号鍵の場合の手順と同様にして暗号鍵データベースDB824aよりIDもしくは第2暗号鍵817に対応する第2復号鍵829を検索し、これを用いて第2暗号デコーダ832において暗号化された課金情報を復号することができます。

10 なお第2暗号エンコーダ831で秘密鍵829を用いてデジタル署名すれば、第2暗号デコーダ832ではユーザーの署名を確認できる。こうして課金センター828は、ユーザーのクレジットカード番号や銀行カード番号や銀行パスワード等の課金情報をインターネットを使っても安全に入手することができる。インターネットのようなオープンなネットワークではセキュリティが問題となるが、このシステムでは、暗号通信用の暗号鍵（公開鍵）もしくはかつデジタル署名の秘密鍵がBCAに記録されているので、暗号通信もしくは認証が確実に行える。このため不正な第3者による不正課金と不正注文を防げるという効果がある。またディスク毎つまりユーザ毎に異なる公開鍵を用いる15 ことができるでの通信の秘密性が向上し、ユーザーの課金情報が第3者に漏洩する可能性が減少する。

ここで、第6図に戻り、パスワードの発行手順とパスワードによる解錠手順を説明する。パスワード発行センター821では、IDとユーザーが解錠したいコンテンツ番号とユーザーの使用許可期間を示す時間情報、の3つの情報に基づき、公開鍵暗号等の演算式を用いたパスワード生成部834でパスワードを生成し、第1コンピュータ909へ送信する。最も簡単な構成例を述べると、第2コンピュータではn番目のコンテンツの暗号を解除する復号鍵ディスクIDと時間情報を混合した情報を公開鍵暗号の公開鍵で暗号化し、これを解く秘密鍵を混合したn番目のパスワード834aをパスワード生成部834で作成し、第1コンピュータ909へ送信する。第1コンピュータは上述の

WO 97/14144

PCT/JP96/02924

## 10

- n番目のパスワードを受信し、秘密鍵でディスクIDと時間情報とn番目のコンテンツの複合鍵を復号する。ここで、ディスクより再生したBCAのID835aと現在の第2時間情報835bと許可されたID833aと第1の時間情報833を照合して一致するかをパスワード演算部836は演算はする。もし一致すれば、許可し、n番目の復号鍵836aを暗号デコーダ837へ出力し、n番目のコンテンツの暗号837aが復号され、n番目のコンテンツ838が出力される。出力される期間は第1時間情報833と第2時間情報835bが一致している間だけに制限される。第1コンピュータ90側では、IDとパスワード835と現在の時間を示す時計836bからの時間情報の3つを情報をパスワード演算部836で演算し、IDと時間情報が正しければ、正しい復号鍵が演算結果として出力されるので、n番目の暗号が暗号デコーダ837で復号もしくは、デスクランブルされて、n番目のコンテンツ838の平文データもしくは、デスクランブルされた映像信号もしくはオーディオ信号が出力される。

- この場合、時計836bの第2時間情報835bがパスワードの第1時間情報と833一致しないと暗号が正しく復号されないので再生はされない。時間情報を用いると、レンタル利用の際に3日間だけ映画を再生できるといった時間限定型のレンタルシステムに応用することが可能となる。

第6図ではブロック図を用いて手順を説明したが、この手順のフローチャートは図16～図23を用いて後で説明する。

- 次に暗号鍵の容量についての工夫を述べる。こうして第7図(a)に示すようにBCAに第1暗号鍵816と第2暗号鍵817の双方を入れることにより、“モール”との商品取引と、“課金センター”との間の代金決済の2つのセキュリティが保たれるという効果が得られる。

この場合、課金センターとのセキュリティに関してはSET等の規格統一が予定されており、RSA1024つまり、128bytesの暗号鍵が、第2暗号鍵領域817

WO 97/14144

PCT/JP96/02924

## 11

aに収容されることになる。すると、BCAは188 bytesしかないため、“モール”との取引の暗号鍵用には60 bytesしか残らない。20バイトの大きさでRSA1024の128バイトと同程度のセキュリティをもつ暗号関数として楕円関数系公開鍵暗号が知られている。

5 本発明では、第1暗号鍵領域816aに楕円関数を用いている。楕円関数はRSA1024と同等のセキュリティが20バイトで得られる。このため、楕円関数を用いることにより188バイトのBCA領域に、第1暗号鍵816と第2暗号鍵717の双方が収容できるという効果がある。

以上述べたように、BCAを光ROMディスクに適用することにより、ディスク固有のID番号、第1と第2暗号鍵、接続のアドレスが記録できる。この場合インターネットを利用した場合に、自動的にモールに接続され、コンテンツの暗号解除による商品流通と、商品購入の認証と秘密保持、代金決済時の認証と機密性の保持等のセキュリティがBCAに暗号鍵が記録されたディスクを配布するだけで、実現する。このため本発明の暗号通信の方法により、従来のようなIDや、暗号鍵をユーザーへ配布するためにICカードやフロッピイや手紙を用いるという作業がセキュリティを落とすことなしに省略でき合理化できるという大きな効果がある。またインターネットの接続アドレスであるURLは固定ではなく、変更される。原盤にはURLが記録されており、このURLに接続すればよいが、変更された時原盤を変更するのは、時間的コスト的に効率が悪い。BCAに変更されたURLを記録しておき、BCAより接続アドレス931が再生された場合のみ原盤の接続アドレスよりBCA接続アドレス931を優先して接続すれば、原盤を新規に作成することなく、変更された接続アドレス931に接続されるという効果がある。

第6図ではBCAに公開鍵の第1号鍵と公開鍵の第1号鍵を記録した場合を示した。

第8図では、BCAに公開鍵の第1暗号鍵816と秘密鍵の第3復号鍵817aの2

WO 97/14144

PCT/JP96/02924

## 12

つを記録した場合と暗号鍵を発生させて暗号通信する場合の2種類の実施例を示す。第6図と同様の手順であるため、違う点のみを述べる。まず、プレス工場では、第1暗号鍵816と第3復号鍵817aがBCAに記録される。第3復号鍵817aは課金センターからの公開鍵で暗号化された暗号の受信に用いる。この場合、受信のセキュリティが向上するという効果がある。

まず、第8図を用いて暗号鍵を生成するより具体的な暗号通信の例を説明する。第1暗号鍵816は公開鍵なので、受信用の第3復号鍵817aをBCAに記録する必要がある。一方BCAは容量が少ない。又公開鍵は処理時間を要する。そこで、第8図では第1コンピュータ836で乱数発生器等で暗号鍵生成部838aで公開鍵の暗号鍵／復号鍵の対、又は共通鍵を生成する。共通鍵の例を述べる。共通鍵K838を第1暗号鍵816と第1暗号エンコーダ842で暗号化し、第2コンピュータ821aへ送る。第2コンピュータでは主復号鍵844を用いて、主暗号デコーダ843で、この暗号を平文化して共通鍵K838aを得る。双方が共通鍵Kをもつので、第2暗号エンコーダ842aと第2暗号デコーダ847aに共通鍵Kを渡すことにより、店からユーザー、つまり第2コンピュータ821aから第1コンピュータ836への暗号通信ができる。当然共通鍵Kを第2暗号エンコーダ827aと第2暗号デコーダ845aに渡すことにより、ユーザーから店つまり第1コンピュータ836から第2コンピュータ821aへの暗号通信も可能となる。公開鍵である第1暗号鍵をBCAに記録し、暗号鍵を生成する方式の効果を述べる。まず、第1暗号鍵の記録だけでよく復号鍵の記録が省略できる。従ってBCAの少ない容量を減らすことがない。次にBCAに復号鍵が記録されているので、セキュリティが向上する。共通鍵の場合、毎回鍵を変えればよい。

演算時間が短いため、処理時間が少なくて済むという効果がある。この場合暗号鍵生成部838aが共通鍵ではなく、公開鍵暗号の暗号鍵と復号鍵の一対を生成した場合暗号鍵を第2コンピュータ821aへ暗号送信し、第2暗号エンコーダ842aの暗号鍵

WO 97/14144

PCT/JP96/02924

## 13

として用い、復合鍵を第2暗号デコーダ847の復号鍵として用いれば処理時間は長くなるが共通鍵に比べてよりセキュリティを高めることができる。処理するCPUの性能が高い場合は公開鍵を使う方が望ましい。公開鍵を新たに生成する場合は、BCAには第1暗号鍵の公開鍵しか記録されないため、セキュリティの問題発生しない。BCAの容量も消費されない。また暗号鍵を変更する必要がないためメンテナンスも容易となる。

5 今度はパスワード発行センター821の第2コンピュータ821aで共通鍵K838aを定義した場合、共通鍵を第3暗号鍵839を用いて第3暗号エンコーダ840で暗号化し、パソコン836へ送信する。パソコン836側ではBCAより再生した秘密鍵である第3復号鍵837を用いて、第3暗号デコーダ841で平文化することにより、10 共通鍵K838bを得る。この場合、秘密鍵である第3復号鍵817aはこのユーザーしかもっていないので、センターからユーザーへの通信の内容が第3者に漏洩することは防止されるという効果がある。この場合のフォーマットを第7図(b)に示す。第3復号鍵839bは梢円関数を用いると20バイトでよいためBCAに収容できる。

次に第9図を用いて、暗号化ディスクにBCAを用いて原盤作成費用を削減する実施例を説明する。

n個例えば、1000本の平文のコンテンツ850があると、各々1~m番目の暗号鍵851を用いて暗号エンコーダ852で暗号化する。この暗号化された第1~m番目のコンテンツ853と1~m番のコンテンツの復号プログラム854aと第2暗号を復号するプログラムである第2暗号デコーダ861aは、原盤に凹凸のピットとして記録された後、1枚の基板に成形され反射膜を形成した後、2枚の基板が貼り合わせられて、光ディスク801が完成する。この時、ディスク1枚目に異なるディスク固有の識別情報、いわゆるとID855とn番目、例えば1番目のコンテンツを解錠するパスワードや復号鍵等の復号情報854を第2暗号エンコーダ860で暗号化した第2暗号を予めBCAに記録する。すると、再生装置ではBCA再生部820より第2暗号が再生さ

れる。BCA以外の通常の記録データが再生されるデータ再生部862よりは第2暗号デコーダ861が再生されるので、これを用いて第2暗号を復号し、ID855aと第n番目のパスワード854aが再生される。暗号デコーダ855bでは、データ再生部862より再生したn番目のコンテンツの復号プログラム854aを用いて、ID855aとパスワード854aを用いて第1暗号を復号し、n番目のコンテンツの平文855cと識別情報855aを得る。パソコンの場合はハードディスク863にコンテンツとIDは記録される。このID855aは、プログラム起動時にネットワーク上に同じIDがないかをチェックし、ネットワークプロテクションを動作させてるので、ソフトの不正インストールが防止できるという副次的效果がある。つまり、原盤1枚に暗号化した1千本のコンテンツを入れ、特定のソフトに対応するパスワード等の復号情報を記録しておけば、実質的に特定の1本のコンテンツの光ROMディスクを作成したのと等価となる。1枚の原盤で1000種類のソフトの原盤をカッティングしたのと同じ効果が得られ、原盤作成費用と手間が削減できるという効果がある。

図10ではRAMディスクに、コンテンツを記録する際にBCAを用いて暗号化する手順を述べる。まず、RAMディスク856よりBCA再生部820により、BCAのデータを再生し、ID857を出力し、インターフェース858a, 858bとネットワークを介して、暗号化部859に送る。暗号化部859ではコンテンツ860をID857を含む鍵で暗号エンコーダ861において暗号化もしくは映像音声信号のスクランブルを行う。暗号化されたコンテンツは記録再生装置に送られ記録回路862によりRAMディスク856に記録される。

次に、この信号を再生する時は、データ再生部865により、主データの復調を行い、暗号化された信号を再生し、暗号デコーダ863において、復号が行なわれる。この時、RAMディスク856のBCA領域から、BCA再生部820により、ID857を含む情報が再生され、暗号デコーダ863に鍵の一部として送られる。この時、正規にコ

WO 97/14144

PCT/JP96/02924

ピーされた場合はRAMディスクに記録された暗号の鍵は正規のディスクIDであり、RAMディスクのIDも正規のディスクIDであるため、暗号の復号もしくはデスクランプルが行なわれ、第n番目のコンテンツの平文864が出力される。映像情報の場合はMP EG信号が伸長されて、映像信号が得られる。

- 5 この場合、暗号化はディスクIDを鍵としている。ディスクIDは世の中に1枚しか存在しないため、1枚のRAMディスクにしかコピーできないという効果が得られる。ここで、もしこの正規のRAMディスクから、別のRAMディスクにコピーした場合、最初の正規のディスクIDであるID1と、別の不正のRAMディスクのディスクIDであるID2とは異なる。不正のRAMディスクのBCAを再生するとID2が再生される。しかし、コンテンツはID1で暗号化されているので、暗号エンコーダ863においてID2で解鍵しようとしても、鍵が異なるため、暗号は復号されない。こうして、不正コピーのRAMディスクの信号が出力されず、著作権が保護されるという効果がある。本発明はDisk ID方式なので正規に1回だけコピーされた正規のRAMディスクはどのドライブで再生しても、暗号が解錠されるという効果がある。ただし、暗号化部859はセンターのかわりに暗号エンコーダを搭載したICカードでもよい。
- 10
- 15

図11図のブロック図と第12図のフローチャートを用いて、コピー防止方法を述べる。ステップ877aでインストールプログラムを動作させる。ステップ877bで張り合わせた光ディスク801より、BCA再生部820より副情報のIDが outputされる。ステップ877dでデータ再生部865より主情報よりコンテンツとネットワークチェックソフト870が再生される。コンテンツとID857はHDD872に記録される。ステップ877cで不正に改ざんされないようID857は特定の秘密の暗号演算を行い、HDD857にソフトIDとして記録される。こうして、パソコン876のHDD872にはコンテンツとともにソフトID873が記録される。ここで第12図のステップ877fのプログラムを起動する場合を述べる。プログラムを起動する時は、ステ

WO 97/14144

PCT/JP96/02924

16

ップ877gにおいて、HDD872のソフトID873を再生し、インターフェース  
875を介して、ネットワーク876の上の別のパソコン876aのHDD872aの  
中のソフトID873aをチェックする。ステップ877hで他のパソコンのソフトI  
D873aと自分のソフトID873が同一番号であるかをチェックし、同一番号であ  
る場合は、ステップ877jへ進み、パソコン876のプログラムの起動を中止するか  
5 画面に警告メッセージを表示する。

他のパソコンのソフトID873aが同一番号でなかった場合は、少なくともネット  
ワーク上にはコンテンツを複数台にインストールした形跡はないため不正コピーはないと  
10 判断し、ステップ877kへ進み、プログラムの起動を許可する。この場合、他のパ  
ソコンへネットワークを介してソフトID873を送信してもよい。このパソコンでは  
各パソコンのソフトIDの重複をチェックすれば不正インストールが検出できる。不正  
があれば、該当するパソコンに警告メッセージを送る。

こうして、BCAにIDを記録し、ネットワークチェックプログラムをピット記録領域  
域に記録することにより、同一ネットワーク上の同一IDのソフトの複数インストール  
15 を防止できる。こうして簡便な不正コピープロテクトが実現する。

図13のように白色の材料からなる書き込み可能な書き込み層850を塗布すること  
により設けることにより、文字を印刷したりペンでパスワード等を書き入れることができる  
だけなく、書き込み層850が厚くなるため光ディスクの基板の損傷を防ぐとい  
う効果も得られる。この書き込み層850の上のBCA領域801aにトリミングで記  
20 録されたBCAデータ849の一部であるディスクID815を平文化し英数字に変換  
した文字851と一般バーコード852を印字することにより、販売店やユーザーがB  
CAを再生装置でよみとることなく、POSのバーコードリーダーや視認でIDの確認  
や照合ができる。視認できるIDはユーザーがパソコン経由でIDをセンターに通知す  
る場合は不要である。しかしユーザーが電話でIDをセンターに口頭で伝える場合は、

WO 97/14144

BCAのIDと同じIDがディスク上に視認できる形式で印刷することにより、ユーザーがIDを目でよみとれるのでパソコンにディスクを挿入することなしにIDをセンターに伝えることができる。図13のフローチャートで光ディスクの製造ステップを説明する。ステップ853dで、原盤よりディスクの成形を行い、ピットの記録された基板を作成する。ステップ853eでアルミ反射膜を作成する。ステップ853fで2枚のディスク基板を接着剤で貼り合わせ、DVDディスク等を完成させる。ステップ853gでスクリーン印刷のラベル印刷をディスクの片面に行う。この時バーコードで原盤に個有の識別情報を記録する。ステップ853hでPOS用バーコードのフォーマットでディスク1枚ごとに異なるID等の識別情報をインクジェットバーコード印刷機や熱転写型バーコード印刷機で印刷する。ステップ853iで、このバーコードをバーコードリーダーでよみ出し、ステップ853jで識別情報に対応したBCAデータをディスクの第2記録領域に記録する。この製造方法であると、BCAを除くPOSバーコードを含む全工程を終えた後にディスク識別情報を確認した上で、BCAデータを記録する。BCAはディスクを再生しないと読めないが、POSバーコードは密度が低いので市販のバーコードリーダーでよみとれる。工場の中のあらゆる工程で、ディスクIDが識別できる。BCAトリミングの前にPOSバーコードでディスクIDを記録しておくことにより、BCAとPOSバーコードの誤記録がほぼ完全に防止できる。

このBCA方式で二次、三次記録もできるBCAの利用方法について述べる。図15に示すようにソフトメーカーでは、工程(2)で示すように海賊版防止マークと照合暗号を二次記録もできる。工程(2)ではディスク1枚ごとに異なるID番号やユーザーとの秘密通信用の暗号鍵を記録したディスク944bを作成しても良い。このディスク944c、944dはパスワードを入力しなくても再生できる。

別の応用として工程(3)では、暗号化やスクランブルしたMPEG映像信号等の情報をディスク944eに記録する。MPEGスクランブルの詳しい動作は説明を省略す

る。ソフト会社では工程（4）においてID番号とスクランブル解除情報を復号するためのサブ公開鍵をBCAで二次記録したディスク844fを作成する。このディスクは単独では再生はできない。工程（5）では、販売店でディスクの代金を受け取った後にサブ公開鍵とペアになっているサブ秘密鍵でパスワードを作成し、ディスクに三次記録する。もしくはパスワードの印刷されたレシートをユーザーに渡す。このあと、ディスク844gはパスワードが記録されているためユーザーが再生可能となる。この方式を用いると、代金の支払われていないディスクを万引きしても映像のスクランブルが解除されないため正常に再生されないため、万引きが無意味になり減るという効果がある。

レンタルビデオ等の店では恒久的にパスワードをBCA記録すると万引きされた場合、  
10 使用されてしまう。この場合は工程（6）に示すように店でBCAをPOSバーコードリーダーでよみとりスクランブル解除のためのパスワードをステップ951gで発行し、ステップ951iでレシートに印刷し、ステップ951jで客に手渡す。客の方は、自宅でステップ951kでレシートのパスワードをプレーヤにテンキーで入力する。ステップ951pで所定の日の間だけ再生される。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみたい時は、電話で、そのソフトのパスワードをステップ951uで通知しステップ951kで入力することにより、ディスクの他のソフトを再生することができる。レンタルビデオ店の例を示したがパソコンソフト店で、暗号化したパソコンソフトを売った時に、POS端末でパスワードを印刷して渡しても良い。

20 図15の工程（5）（6）のセル販売店、レンタル店における動作を図14を用いてより具体的に説明する。セル販売店ではソフトメーカーから暗号やスクランブルがかったディスク944fを受け取り、ユーザーからの入金を確認するとバーコード記録装置945よりディスク944fのID番号、サブ公開鍵のデータをPOS端末946経由でパスワード発行センター952に送信する。小規模なシステムの場合パスワード発

WO 97/14144

PCT/JP96/02924

19

行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはPOS端末の中においても良い。パスワード発行センターはステップ951qでディスクID番号と時間情報を入力し、ステップ951sで演算を行い、ステップ951tで、サブ秘密鍵を用いて暗号化し、ステップ951gでパスワードを発行しネットワーク948とPOS端末84

5 6を介してBCAバーコード記録装置945にパスワードを送り、記録されたディスク944gが客に渡される。このディスク944gは、そのまま再生できる。

次にレンタル店やパソコンソフト店の場合、まず暗号やスクランブルの解除されていないROMディスク944fを店頭に陳列する。客が特定のROMディスク944fを指定した場合、うずまき型にスキャンする回転型の光学ヘッド953を内蔵した円形バーコードリーダ950を手に持ち透明ケース入りのディスク900の中心におしつけることにより、ディスク944fの無反射部915による反射層のバーコードを読み取り、ディスクID番号を読み取る。ディスクIDの商品バーコードを図13の852のように印刷することにより通常のPOS端末のバーコードリーダーで読み取ることが出来る。原盤に予め記録されプレスされた円形バーコードから読み取っても良い。これらのディ

10 15 スクIDを含む情報はPOS端末946により処理され、料金がクレジットカードから決済されるとともに、前述のようにID番号に対応したパスワードがステップ951gにおいてパスワード発行センターから発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ951rで用いたように日付情報を加えて、ディスクID番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しな

20 いため、例えば3日間の貸し出し期間をパスワードの中に設定できるという効果がある。

さて、こうして発行されたスクランブルのためのパスワードはステップ951iにおいて、貸出日、返却日、レンタルのタイトル料金とともにレシート949に印刷され客にディスクとともに渡される。客はディスク944jとレシート949を持ち帰り、ステップ951kでパスワードを図6の第1コンピュータ909のテンキー入力部95

4に入力することによりパスワード835はID番号835aと演算されて暗号デコーダ837に入力され、復号鍵を用いて平文化される。正しいパスワードである場合のみ暗号デコーダ837でプログラムのデータをデスクランブルし、映像出力を出力させる。

この場合、パスワードに時間情報が含まれている場合、時計部836bの日付データ

- 5 と照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するID番号とともにメモリ755の不揮発メモリ755aにストアされ、ユーザーは一度パスワードを入力すると2度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

第16図を用いてソフトが暗号データとして記録されたディスクのソフトの復号方法

- 10 を詳しく説明する。

ステップ865は暗号データと個別IDのユーザーへの配布の全体フローを示す。まず、ステップ865aでは、1枚の原盤のROM領域に、秘密の第1暗号鍵で暗号化されたmヶのデータと、暗号化されたmヶのデータを復号するプログラムを記録する。ステップ865bでは、原盤より基板を成形し、反射膜を附加した2枚の基板を貼り合わせて完成ROMディスクを複数枚、作成する。ステップ865cでは、完成ディスクの書換できない副記録領域(BCAとよぶ)に、暗号化データの復号に必要な復号情報(プレスしたディスク毎に異なるディスク識別情報 and / or 暗号データの復号鍵)をROM領域と異なる変調方法で記録する。ステップ865dでは、ユーザーは配布されたディスクを再生し、希望する暗号化データnを選択し、復号処理を始める。

- 20 ステップ865eで、ユーザーの第1コンピュータで、ROM領域から暗号化データと復号プログラムを再生し、副記録領域(BCA)から、復号情報を読み出す。ステップ865fで、オンラインで第2復号情報を得ない場合は図17のステップ871aで、ID等の復号の補助情報を画面上に表示する。ステップ871bで、ユーザーはIDに対応するパスワード等の第2復号を入手し、第1コンピュータに入力する。ステップ8

71cで、ディスク識別情報と第2復号情報と暗号化データnを用いて公開鍵系暗号関数の特定の演算を行う。ステップ871dで結果が正しければ、ステップ871fでn番目のデータが平文化され、ユーザーはデータnのソフトを動作させることができる。

次に図18のフローチャートを用いて、BCAを用いたインターネット等で必須な暗号通信の方法を述べる。ステップ868は、ユーザーへ通信プログラムと通信暗号鍵を配布する方法のルーチンである。まず、ステップ868aで、1枚の原盤のROM領域に少なくとも通信プログラムや接続情報を記録する。ステップ868bで、原盤より基板を成形し、2枚の基板を貼り合わせて完成ROMディスクを複数枚作成する。ステップ868cで、完成ディスクの書換できない副記録領域(BCA)に、プレスしたディスク毎に異なるディスク識別情報と暗号通信用暗号鍵を記録する。場合により第2コンピュータの接続アドレス、もしくは/かつ暗号通信用復号鍵をROM領域と異なる変調方法で記録する。ステップ868dで、ユーザーの第1コンピュータで、ROM領域から通信プログラムと暗号化プログラムを再生し、副記録領域から、ディスク識別情報と通信用暗号鍵を読み出す。第19図に進みステップ867aで、BCA領域に接続アドレスがある場合は、ステップ867bで、BCA領域のURL等の接続アドレスに基づき第2コンピュータに接続し、接続アドレスがない場合はステップ867cのROM領域の接続アドレスのコンピュータに接続する。ステップ867dで、送信データが入力され、ステップ867eで、BCA領域に暗号通信用暗号鍵がある場合はステップ867gでBCA領域の暗号通信用暗号鍵を用いて、送信データを暗号化し、第3暗号を作成する。また、ない場合はステップ867fでROM領域又はHDDの暗号通信用の暗号鍵を用いてデータを暗号化し、第3暗号を作成する。

次に第20図では第2コンピュータ910から受信した暗号の復号鍵の生成ルーチンをステップ869で述べる。まず、第1コンピュータではステップ869aで、通信復号鍵が必要な場合は、ステップ869bへ進み、BCAに通信用復号鍵があるかどうか

をチェックし、復号化鍵がない場合は、ステップ 869c で ROM 領域から再生した暗号鍵／復号鍵の生成プログラムを用いてユーザーのキー入力もしくは乱数発生器のデータと ROM 領域から再生した第 2 暗号器により一対の第 2 通信暗号鍵／第 2 通信復号鍵を新たに生成する。ステップ 869d で、“第 2 通信暗号鍵もしくは／かつユーザーデータ” を BCA に記録された通信暗号鍵と ROM 領域から再生して得た暗号化ソフトを用いて暗号化した第 4 暗号を作成する。ステップ 869e で、第 4 暗号と、ディスク識別情報もしくは／かつユーザー アドレスを、ディスクから再生して得た接続アドレスの第 2 コンピュータに送信する。第 2 コンピュータの処理としては、ステップ 869f で、第 4 暗号とディスク識別情報とユーザー アドレスを受信する。ステップ 869g では、  
10 復号鍵データベースから、ディスク識別情報と対になった通信復号鍵を選択し、これを用いて第 4 暗号を復号し、第 2 通信暗号鍵の平文を得る。ステップ 869h で、第 2 通信暗号鍵を用いて、ユーザー データの一部を含むサーバーのデータを暗号化した第 5 暗号を第 1 コンピュータへインターネット 908 で送信する。ステップ 869i で、第 5 暗号（とディスク識別情報）を受信し前述の第 2 通信復号鍵と ROM 領域に記録された  
15 復号関数を用いて復号し、前述のサーバーデータの平文を得る。こうして、第 20 図のステップ 869 の方式で、第 1 、第 2 コンピュータ間で双方向の暗号通信が実現する。

第 21 図のステップ 870 では課金情報の受信ルーチンについて説明する。ステップ 870a で、課金情報を入力する場合は、課金通信用の公開鍵暗号の第 3 暗号鍵を第 2 コンピュータへ要求する。ステップ 870b では、第 2 コンピュータが、第 3 コンピュータへ第 3 暗号鍵を要求する。やりとりのステップは省略するが、第 3 コンピュータ 911 は ID と第 3 暗号鍵を第 2 コンピュータ 910 へ送信する。ステップ 870c で、第 2 コンピュータは ID と第 3 暗号鍵を受信し、ステップ 870e で、第 3 暗号鍵を第 2 通信暗号鍵等を用いて暗号化した第 7 暗号を第 1 コンピュータへ送信する。第 1 コンピュータではステップ 870f で、第 7 暗号を受信し、ステップ 870g で、前述の第

2通信復号鍵を用いて、受信した第7暗号を復号し、第3暗号鍵（公開鍵関数の公開鍵）を得る。ステップ870hでは、必要に応じて第3暗号鍵をHDDに記録する。これは次回の送信時に利用する。ステップ870iで、クレジットカード番号や決済用パスワード等の機密値が高い課金情報を入力する場合は、ステップ870jで第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第2コンピュータ経由で第3コンピュータへ送る。第2コンピュータは、ステップ870kで第8暗号を受信し、第3コンピュータへ再転送する。第3暗号の復号鍵は金融機関である第3コンピュータ912しか持っていないため、第2コンピュータの電子商店では解読できない。第3コンピュータではステップ870mで、暗号鍵データベースからディスク等の識別情報を用いて第3暗号鍵に対応した第3復号鍵を探しだし、公開鍵暗号の秘密鍵である第3復号鍵で第8暗号を復号し、課金情報の平文を得る。ステップ870nでは、ユーザーの信用情報や預金残高等の金融情報から、代金が回収できるかをチェックし、ステップ870pでは、調査結果を第2コンピュータへ通知する。第2コンピュータいわゆる電子商店はステップ870qで代金の回収可能かどうかを判定して、不能と判断すれば、ステップ870rで、商品の発送や暗号ソフトを復号する鍵の送付をしない。代金回収可能と判断した場合、図16のような鍵提供システムの場合、ステップ870sへ進み、暗号ソフトの復号鍵つまり商品をインターネット908で、ユーザーの第2コンピュータに送信する。第1コンピュータでは、ステップ870tで、暗号ソフトの復号鍵を受信して、ステップ870uでn番目の暗号化ソフトの暗号を解除して、ステップ870wで、ソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

この図21のステップ870の方式は課金情報という高いセキュリティが要求される第3暗号鍵の公開鍵を第3コンピュータつまり、金融機関に、必要に応じて要求し発行させる。BCAに予め記録しておかなくてもよい。従って第3暗号鍵にRSA2048の256バイトのさらに強力なRSA系の暗号鍵をBCAの容量を消費することなしに

用いることができるという効果がある。さらに全てのディスクのBCAに予め記録する必要がないので、第3暗号鍵の発行総数が少なくなり、第3暗号鍵の演算に要するコンピュータのCPUタイムが減る。また、第3暗号がBCAにないため、公開されないため、セキュリティが若干向上する。この場合のBCAの役割は、第19、20図のよう

- 5 に、RSA 1024グレードの暗号鍵による秘密通信ディスクの識別情報の記録である。BCAディスク1枚あれば、第2コンピュータとの暗号通信が実現するため効果は高い。

次に第22図を用いて、BCAに通信暗号鍵と通信復号鍵の双方を記録した時の、暗号通信のステップ872を説明する。ステップ872gで、第1コンピュータ909ではBCAから再生して得た通信暗号鍵でユーザーデータを暗号化した第9暗号と、原盤

- 10 作成時にROM領域に記録された基本識別情報と、BCA領域に記録されたディスク識別情報を第2コンピュータ910へ送信する。第2コンピュータでは、ステップ872bで、第9暗号とディスク識別情報と基本識別情報を受信する。ステップ872cで、復号鍵データベースからディスク識別情報と対になった通信復号鍵を検索し、第9暗号

- 15 を復号し、ユーザーデータの平文を得る。ステップ872eで、ディスク識別情報に対応した第2暗号鍵を暗号鍵データベースから選別し、この第2暗号でサーバーデータと

図21で述べた手順で第3コンピュータから受信した第3暗号鍵を暗号化した第10暗号を第1コンピュータへ送信する。第1コンピュータではステップ872fで、第10

- 20 暗号を受信し、ステップ872gで、BCAに記録された前述の通信用第2復号鍵を用いて、受信した第7暗号を復号し、サーバーデータと第3暗号鍵(公開鍵関数の公開鍵)

の平文を得る。ステップ872hで必要に応じて第3暗号鍵をHDDに記録する。ステップ872iで課金情報を入力する場合は、ステップ872jへ進み、第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第1暗号を第2コンピュータ経由で第3コンピュータへ送る。第2コンピュータでは、ステップ872mで、第11暗号を第3コンピュータへ再送信する。第3コンピュータでは、ステップ872nで、第3暗号鍵デ

WO 97/14144

PCT/JP96/02924

25

- ータベースからディスク等の識別情報と対になった第3暗号鍵を探しだし、第8暗号を復号し、課金情報の平文を得る。ステップ872nでは、ユーザーへの課金回収の可能性のチェックを行い、ステップ872pで調査結果を第2コンピュータへ送信する。第2コンピュータではステップ872qでユーザーが課金の回収が可能かどうかをチェックする。代金回収可能と判断した場合図1-6のような鍵提供システムの場合、ステップ872sへ進み、暗号ソフトの復号鍵、つまり商品をインターネットでユーザーの第2コンピュータに送信する。第1コンピュータではステップ872tで暗号ソフトの復号鍵を受信して、ステップ872uでn番目の暗号化ソフトの暗号を解除してステップ872wでソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。
- 10 第22図のステップ872の方式の効果の特長は、暗号鍵と復号鍵の双方がBCA領域に記録されているため、第2コンピュータからの受信に必要な復号鍵や暗号鍵の送信が必要ないという点である。BCAの容量は最大188バイトであるので、公開鍵等の暗号関数なら、RSA512で64バイト2ヶで、128バイトで済むので記録できる。RSA512にグレードの双方向の暗号化が可能となる。椭円関数なら第7図に示すように7~8ヶ収容できるため、効果はさらに高い。

第23図を用いて、BCAに第1暗号鍵と第3暗号鍵を予め記録した場合の動作と効果について述べる。なお、第22図のステップ872a~872wと第23図のステップ873a~873wは、ほぼ同じ構成なので違うステップだけを説明する。

まず、課金情報等の金融情報のセキュリティを守る第3暗号鍵がBCAに記録されているので、ステップ873eにおいて第2、第3コンピュータは第3暗号鍵の生成と送信は不要となる。ステップ873e、873f、873gにおいて第12暗号の送受信が行われる。また、ステップ873jにおいてはBCA領域から第3暗号鍵を読み出し、ユーザーの課金情報を第2コンピュータ経由で第3コンピュータへ送る。第23図の方法は、第3暗号鍵の生成、送受信が全く不要となるため、手順が簡単になるという

効果がある。

さて、電子決済システムの場合、課金センターはクレジット開始や同様、通常、複数個存在する。従って、当然公開鍵である第3暗号鍵は複数個必要となる。第7図 (b)

5 RSA暗号関数を使うとRSA1024グレート以上つまり128バイト以上必要であるので、BCAの188バイトには1ヶしか第3暗号鍵8.1.7 bは入らない。しかし、近年登場した楕円関数系暗号鍵（楕円暗号）は小容量でRSAと同等のセキュリティが得られる。近年ではRSA関数のRSA1024が金融情報のセキュリティの最低基準となっている。RSA関数だと128バイト必要であるが、同等のセキュリティを得るのに、楕円暗号であると、20~22バイト程度で良いといわれている。従って第7図 (c)に図示するように金融情報を取り扱う第3暗号を複数ヶ、最大10  
10 7~8つBCAに収容できる。楕円暗号を使うことにより、現実的に必須である複数の金融センターに対応した、BCA応用の電子決済システムが実現する。第3暗号に的を絞って説明したが、第1暗号鍵の公開鍵に用いても、複数の電子商店との間の高いセキュリティが保たれるため楕円暗号の効果は同様である。

15 次に第24図を用いて、図10で説明したBCAを用いたRAMディスク記録再生装置に関して更に詳しく述べる。1つの実施例としていわゆるPay per ViewシステムにおけるRAMディスクへの記録手順を述べる。まず、CATV会社等のソフト会社は番組送信器8.8.3において、映画ソフト等のコンテンツ8.8.0を第1暗号鍵8.8.2を用いて第1暗号器において暗号化し、第1暗号9.0.0を生成し、各ユーザーのCATVデコーダの如きデコーダ8.8.6に送信する。デコーダ8.8.6側ではネットワークを介して鍵発行センター8.8.4へ特定の番組の要求を送ると、鍵発行センター8.8.4は、特定のソフトでかつ特定のデコーダのシステムID番号かつ特定の時間制限情報9.0.3に対するスクランブル解除キーの如き第1復号情報でかつ、RAMディスクへの記録許可カード9.0.1が含まれている第1復号情報8.8.5aを第1デコーダ8.8.6の第1復号

部887へ送信する。第1復号部887はシステムID888と第1復号情報885aより、第1暗号900を復号し、映像信号の場合は、一旦デスクランブルされた信号がさらに別の暗号でコピー防止用のスクランブルされた信号が第3暗号出力部889から出力され、一般TV899で、元のTV信号がコピーガードされているか観聽できる。

- 5 ここで、記録許可コード9-01-aがNOの場合は、RAMディスク894に記録できない。しかし、OKの場合はRAMディスク894の1枚に限り記録できる。この方法を説明する。

デコーダ886では、ICカード902が挿入され、RAMレコーダのRAMディスク894のBCAをBCA再生部895が読み取りディスクID905がICカード902に送られる。ICカード902はディスクIC905とデコーダ886から得た現在の時間情報904と記録許可コード901aをチェックし、第3暗号出力部889と双方向でシェイクハンド方式のコピーチェック907を行い、記録許可コードとコピーチェックがOKならICカード902の中の第2副暗号器891は第2暗号鍵906を発行する。第2暗号器890において、第3暗号は再暗号化されて特定の1枚のディスクのディスクIDでコンテンツ880が暗号化された第2暗号が生成され、RAMレコーダ892に送られ記録手段893において8-15や8-16変調を用い、第1変調部により変調され、レーザにより、RAMディスク894の第1記録領域894aに第2暗号912が記録される。こうして、RAMディスク894のデータは特定のディスクIDの番号で暗号化されている。

20 次にこのディスクを通常の再生手段896で再生信号を8-16変調の第1復調部896aで復調するとコンテンツの第2暗号が出力される。第2復号器897は複数の第2復号鍵898a、898b、898cをもつ。これは各CATV局等の番組供給会社毎に異なる各々のICカードの暗号鍵に対応した復号鍵をもつことになる。この場合、デコーダ886もしくはICカード902の復号鍵識別情報は記録時に第1記録領域8

9 4 aに記録されている。再生装置では、第1記録領域8 9 4 aから復号鍵識別情報9 1 3を読み出し、復号鍵選別手段9 1 4により復号鍵8 9 8 a～8 9 8 zのうちからを元に各々の暗号鍵に対応した、第2復号鍵8 9 8 aを自動的に選択し、ディスクID 9 0 5 aを一つの鍵として、第2暗号は第2復号器8 9 7において復号される。特定の復号鍵の入ったICカードを用いてもよい。映像の場合TV 8 9 9 aにてデスクランブルされた正常な映像が得られる。

図24のシステムでは、各ユーザーの自宅のデコーダに挿入したICカードにディスクID 9 0 5を送り、画像データ等を暗号化するので、ソフト会社8 8 3は各ユーザーに配信するコンテンツの暗号を個別に変える必要がない。従って、衛星放送やCATVのように大量の視聴者にペイパービューのスクランブル映像を放送する場合に、各ユーザー毎にRAMディスク1枚だけに記録することを許可する効果がある。

図24のシステムで1枚のディスクに記録すると同時に、2枚目つまり他のディスクIDのRAMディスクに不正にコピーつまり記録しようとするとBCAの場合2層ディスクを用いているのでディスクIDを改ざんすることができないため、同時に2枚目のディスクへの不正コピーは防止される。次に別の時間帯に擬似的な記録許可コード9 0 1 aや第3暗号をデコーダやICカードに送信し、特定のディスクIDでデータは暗号化されている。別のディスクIDのRAMディスクに記録することが考えられる。こうした不正行為にも、ICカードの中のデコーダ時間情報管理部9 0 2が鍵発行センタ－8 8 4の時間制限情報9 0 3やコンテンツの時間情報の時間とデコーダの中の時間情報部9 0 4 aの現在の時間とを比較して、時間が一致しているかをチェックし、OKならICカード9 0 2は第2暗号演算器9 9 0の暗号化を許可する。

この場合、第2暗号器8 9 0と第1復号部8 8 7が双方向でチェックデータを交信するシェイクハンド方式の時間チェック方式でもよい。

シュークハンド方式の場合、I Cカードを含む第2暗号演算器890と、第1復号部887と第3暗号部889は双方向で、暗号データを確認しあう。このためコンテンツの送信時間と同一でない別の時間帯の不正コピーは防止される。)

こうして各ユーザーのもつデコーダ886においては世の中に1枚しか存在しない特定のディスクIDのRAMディスク894の1枚のみに、ソフト会社のコンテンツが記録される。そして、このディスクはどのRAMディスク再生機でも再生できる。図24の方式でRAMディスクに記録する場合でもソフト会社の著作権が守られると言う効果がある。

なお本文の図の説明では、暗号エンコーダで暗号化、暗号デコーダで復号化を説明したが、実際はCPUの中のプログラムである暗号アルゴリズム及び復号アルゴリズムを用いる。

#### 産業上の利用可能性

このように、光ディスクのBCA領域にIDや暗号の暗号鍵や復号鍵を予め記録しておくことにより、暗号化されたコンテンツの暗号解除がより簡単な手順で実現する。また通信の機密性が従来の登録手続きなしで実現する。ネットワークチェックプログラムをコンテンツに収納しておくことにより、同一ネットワーク上の同一IDのソフトの複数インストールを防止できる。このようにセキュリティ向上の様々な効果がある。

WO 97/14144

PCT/JP96/02924

## 請求の範囲

1. 主情報が微小な凹凸であるピットによって第1変調方式で記録された光ディスクの第1記録領域の所定部分において、反射膜を半径方向に長い形状でかつ複数個、部分的に除去することにより前記第1の変調方式と異なる第2変調方式で副情報が記録されている第2記録領域を備えた光ディスクであって、前記副情報に個々の光ディスクを識別するための第1識別情報が記録され、前記第1識別情報もしくは／かつ所定のパスワードを用いて使用可能となる不許可部分が前記主情報の中に記録されていることを特徴とする光ディスク。
- 10 2. 光ディスクは、再生型光ディスクであることを特徴とする請求項1記載の光ディスク。
3. 所定のパスワードは、第1の識別情報を用いて所定の演算を行って求めることを特徴とする請求項1または2記載の光ディスク。
4. 副情報に個々の光ディスクを識別するための第1識別情報に加えて、暗号の暗号鍵もしくは／かつ暗号の復号鍵が記録してある請求項1または2記載の光ディスク。
- 15 5. 第1変調方式として8-16変調方式を行い、第2変調方式としてフェーズエンコーディング変調方式を用いたことを特徴とする請求項1または2記載の光ディスク。
6. 主情報が微小な凹凸であるピットによって第1変調方式で記録された光ディスクの第1記録領域の所定部分において、反射膜を半径方向に長い形状でかつ複数個、部分的に除去することにより前記第1変調方式と異なる第2変調方式で副情報が記録されている第2記録領域を備えた光ディスクであって、前記副情報に個々の光ディスクを識別するための第1識別情報と暗号の暗号鍵もしくは／かつ暗号の復号鍵が記録され、前記第1識別情報もしくは／かつ所定のパスワードを用いて使用可能となる不許可部分が前記主情報の中に記録されている光ディスクを再生するステップと、前記副情報より前記第

1 識別情報を再生するステップと、前記第1識別情報もしくは／かつ前記所定のパスワードとを用いて、前記不許可部分を使用可能とし出力するステップを含むことを特徴とするプログラム使用許可方式。

7. 所定のパスワードは、第1の識別情報を用いて所定の演算を行って求めることを特  
5 徴とする請求項6記載のプログラム使用許可方式。

8. 主情報が微小な凹凸であるピットによって第1変調方式で記録された光ディスク  
の第1記録領域の所定部分において、反射膜を半径方向に長い形状でかつ複数個、部分  
的に除去することにより前記第1の変調方式と異なる第2の変調方式で副情報を記録さ  
れている第2記録領域を備えた光ディスクであって、前記副情報に個々の光ディスクを  
10 識別するための第1識別情報かつ暗号の第1暗号鍵もしくは／かつ暗号の復号鍵が記録  
してある光ディスクを、第1コンピュータにおいて再生し、前記第1識別情報と前記第  
1の暗号鍵を前記副情報より読み出すステップと、前記第1暗号鍵と暗号アルゴリズム  
を用いて第1データを暗号化した第1暗号を得るステップと、前記第1暗号を前記第1  
コンピュータの通信手段からネットワークを介して、第2コンピュータに送信するステ  
15 ップを有することを特徴とする暗号通信方式。

9. 暗号アルゴリズムを主情報から読み出すことを特徴とする、請求項8載の暗号通信  
方式。

10. 第1コンピュータにおいて、光ディスクの第1記録領域から主情報を再生するス  
テップと、第2記録領域から個々の光ディスクを識別するための第1識別情報かつ暗号  
20 の第1暗号鍵もしくは／かつ暗号の復号鍵を含む副情報を再生するステップと、前記第  
1コンピュータの第1データを、副情報の中の第1暗号鍵を用いて、暗号アルゴリズム  
により暗号化し第1暗号を作成するステップと、特定の接続アドレスの第2コンピュー  
タへネットワークを介して接続し前記副情報の中の第1識別情報と前記第1暗号を送信  
するステップと、前記第2コンピュータにおいて前記第2識別情報と前記第1暗号を受

信するステップと、第1復号鍵と第1識別情報の対応関係が格納されている第1復号鍵データベースより受信した前記第1識別情報に対応する暗号の復号鍵である第1復号鍵を選択するステップと、前記第1復号鍵に基づいて、前記第1暗号を復号し、前記第1データを得るステップを有することを特徴とする暗号通信方式。

- 5 1-1. 第1コンピュータにおいて、暗号鍵を生成する第1暗号生成手段により第2暗号鍵と、前記第2暗号鍵と対をなす第2復号鍵を生成するステップと、前記第1コンピュータにおいて第1暗号鍵を用いて前記第2暗号鍵を暗号化した第3暗号を得るステップと、前記第3暗号を第2コンピュータに送信するステップをもつことを特徴とする請求項10記載の暗号通信方式。
- 10 1-2. 第2コンピュータにおいて、受信した第3暗号を第1復号鍵を用いて復号し、第2暗号鍵の平文を得るステップと、前記第2暗号鍵で、第2データを暗号化した第4暗号を得るステップと前記第4暗号を第1コンピュータに送信するステップを有することを特徴とする請求項11記載の暗号通信方式。
- 15 1-3. 公開鍵系暗号を含む副情報から、公開鍵系暗号の2つ以上の暗号鍵もしくは／かつ復号鍵を再生するステップにおいて、前記暗号鍵もしくは復号鍵の鍵のうち少なくとも1つは梢円関数暗号を用いたことを特徴とする請求項8記載の暗号通信方式。
- 1-4. 副情報に第2コンピュータの接続アドレス情報を含む光ディスクを用いて、前記副情報から前記接続アドレスを再生するステップを含むことを特徴とする請求項8記載の暗号通信方式。
- 20 1-5. 光ディスクの第1記録領域の記録層にレーザー光を光学レンズを用いて照射することにより、主情報を第1変調方式で変調して記録する記録装置において、記録する前に第2変調方式で第1識別情報かつ暗号の第1暗号鍵もしくは／かつ暗号の復号鍵が記録された第2記録領域の副情報を再生し、前記第1識別情報もしくは／かつ第1暗号鍵と特定の暗号アルゴリズムを用いて主情報を暗号化した主暗号を作成し、前記主暗

号を前記第1の記録領域の記録層に前記第1の変調方式で記録することを特徴とする光ディスク記録装置。

16. 第1データが第2暗号アルゴリズムで暗号化された第2暗号と、前記第1データを光ディスクに記録することを許可する記録許可情報とを受信部で受信し、前記第2暗

5 号を第2復号手段により復号した第2復号情報を得るとともに、暗号演算手段において前記第2暗号アルゴリズムとは違う第1暗号アルゴリズムと副情報を用いて、前記第2復号情報を暗号化した主暗号を生成し、前記記録許可情報がある場合のみ光ディスクの第1記録領域に前記主暗号を記録することを特徴とする請求項15記載の光ディスク記録装置。

10 17. 演算器の入ったICカードを装着し、前記ICカードに副情報をディスクを識別する第1識別情報を入力し、前記第1識別情報を前記演算器で演算し、演算結果を前記ICカードより暗号演算手段に入力させ、第2復号信号を暗号化した主暗号を得て、前記主暗号を光ディスクに記録することを特徴とする請求項16記載の光ディスク記録装置。

15 18. 第1データが第1識別情報を用いて、暗号手段により暗号化された主暗号が第1記録領域に第1変調方式で記録された光ディスクを光ヘッドと第1復調手段により読み出すとともに、前記光ディスクの第2記録領域に第2変調方式で記録された副情報を前記光ヘッドと第2復調手段により再生し、前記副情報の中の第1識別情報もしくは前記第1識別情報に特定の演算を行った第1副識別情報を用いて前記主暗号を復号手段により復号することにより、前記第1データを得ることを特徴とする光ディスク再生装置。

20 19. 第1復調手段の変復調方式として8-16変復調方式を用い、第2復調手段の復調方式としてフェーズエンコーディング復調方式を用いたことを特徴とする請求項18記載の光ディスク再生装置。

20. 復号手段はnヶの復号鍵をもち、光ディスクの主情報より再生した復号鍵識別情

報に基づいて前記 $n$ ヶのうち、特定の1ヶの復号鍵を選択することを特徴とする請求項

18記載の光ディスク再生装置。

21. 第1コンピューターをネットワークを介して特定のアドレスの第2コンピュータに接続するステップと、副情報の中のディスクを識別するための第1識別情報を前記第5記載の光ディスク再生装置に送信するステップと、前記第2コンピュータにおいて、前記第1識別情報に特定の暗号演算を行い、得たパスワードを前記第1コンピューターに送信するステップと、前記第1コンピューターにおいて前記パスワードと前記第1識別情報を復号演算部において演算を行い、得た第2復号コードを暗号デコーダに送るステップと、前記暗号デコーダが前記第2復号コードを用いて、前記光ディスクの主情報中の不許可部分を使用可能とするステップをもつことを特徴とする請求項6記載のプログラム使用許可方式。

22. 主情報が微小な凹凸であるピットによって第1変調方式で記録された光ディスクの第1記録領域の所定部分において、反射膜を部分的に除去することにより、前記第1変調方式とは異なる第2変調方式で副情報が重ね書きされている第2記録領域を備えた光ディスクであって、前記副情報に個々の光ディスクを識別するための第1識別情報が記録してあるとともに、前記主情報の中に第1プログラムおよび前記第1プログラムを第1コンピューターの中のハードディスクにインストールするインストールプログラムと通信プログラムが記録してある光ディスクを第1コンピューターが再生するステップと、前記副情報より前記第1識別情報を再生するステップと、前記第1プログラムを前記ハードディスクにインストールするステップと、前記第1識別情報もしくは前記第1識別情報に特定の演算を行った第1副識別情報を前記ハードディスクに記録するステップと、インストールした前記第1プログラムの起動、もしくは特定の動作時に、前記通信プログラムは前記第1識別情報もしくは前記第1副識別情報を、前記第1コンピューターにネットワークを介して接続された第2コンピューターに送信するステップ、もしくは前記第

2コンピュータのハードディスクの中の第1識別情報に対応する第2識別情報もしくは第2識別情報に特定の演算を行った第2副識別情報を前記ネットワークを介して、チェックするステップと、前記第1識別情報と前記第2識別情報の一致もしくは、前記第1副識別情報と前記第2副識別情報の一致があった時には前記第1プログラムの特定の動作を制限、もしくは特定の動作を追加するステップを含むことを特徴とするプログラムの不正インストール検出方式。

23. 主情報が微小な凹凸であるピットによって第1変調方式で記録された光ディスクの第1記録領域の所定部分において、反射膜を半径方向に長く、かつ裸眼では情報をよみとれないバー形状に部分的に除去することにより、前記第1変調方式とは異なる第2変調方式でかつ前記主情報よりも低い記録密度で副情報が重ね書きされている第2記録領域を備えた光ディスクであって、前記副情報に個々の光ディスクを識別するための第1識別情報が記録してあるとともに、前記光ディスクの第1記録領域の主情報の中に第1データが記録され、かつ、前記第1識別情報と特定の対応関係にあるデータが商品バーコード用リーダーでよみとれる商品バーコードとして印刷されていることを特徴とする光ディスク。

24. 商品バーコードは光ディスクの再生面と反射側の面に印刷されていることを特徴とする請求項23記載の光ディスク。

25. 主情報が微小な凹凸であるピットによって第1変調方式により記録された光ディスクの第1記録領域の所定部分において、反射膜を部分的に除去することにより、前記第1変調方式とは異なる第2変調方式で副情報が重ね書きされている第2記録領域を備えた光ディスクであって、副情報に個々の光ディスクを識別するための第1識別情報が記録してあるとともに、前記光ディスクの第1記録領域の主情報の中に使用を許可されていない不許可部分を含むとともに、前記第1識別情報もしくは前記第1識別情報と特定の関係にある第1副識別情報が商品バーコード用リーダーで読みとり可能なバーコ

WO 97/14144

PCT/JP96/02924

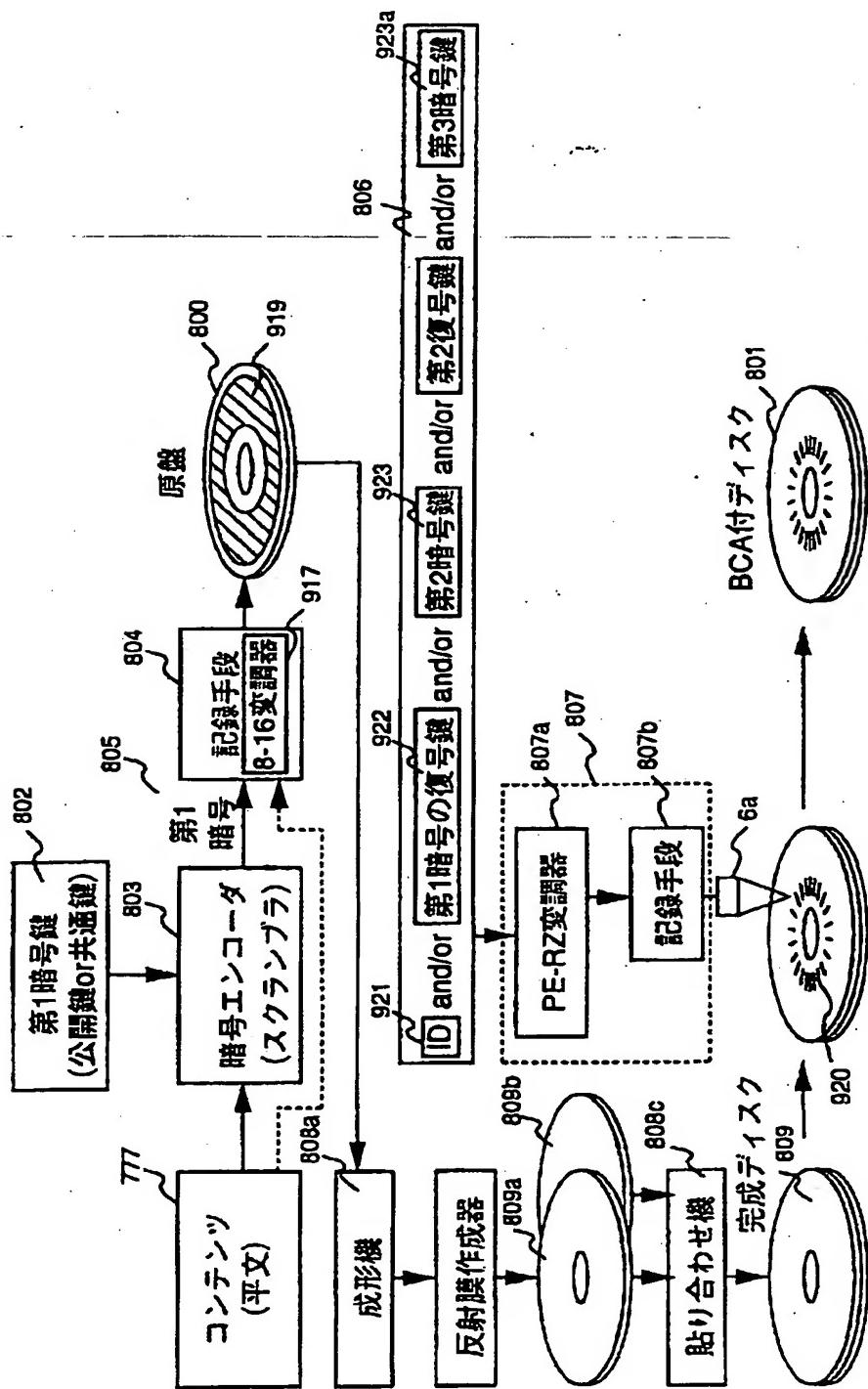
ドが印刷された光ディスクから、第1コンピュータにおいて前記商品バーコード用リーダーを用いて前記第1識別情報もしくは前記第1副識別情報を読みとるステップと、前記第1識別情報もしくは前記第1副識別情報をネットワークを介して、第2コンピュータに送信するステップと、前記第2コンピュータで、前記第1識別情報に基づき、暗号演算を行い前記不許可部分の使用を許可する許可情報を作成するステップと、前記許可情報を前記第1コンピュータへ送信するステップと、前記第1コンピュータで前記許可情報を印刷手段により、用紙に印刷するステップを有することを特徴とする光ディスク中の第1データのプログラム使用許可方式。

26. 主情報が微小な凹凸であるピットによって記録された光ディスクの第1記録領域の所定部分において、反射膜を半径方向に長い形状でかつ複数個、部分的に除去することにより前記ピット上に前記主情報と周波数分離できるような低い周波数帯域で副情報を重ね書きした第2記録領域を備えた光ディスクであって、前記副情報を個々の光ディスクを識別するための第1識別情報が記録され、前記第1識別情報もしくは／かつ所定のパスワードを用いて使用可能となる不許可部分が前記主情報の中に記録されていることを特徴とする光ディスク。

27. 光ディスクは、再生型光ディスクであることを特徴とする請求項26記載の光ディスク。

28. 所定のパスワードは、第1の識別情報を用いて所定の演算を行って求めることを特徴とする請求項26または27記載の光ディスク。

1/27

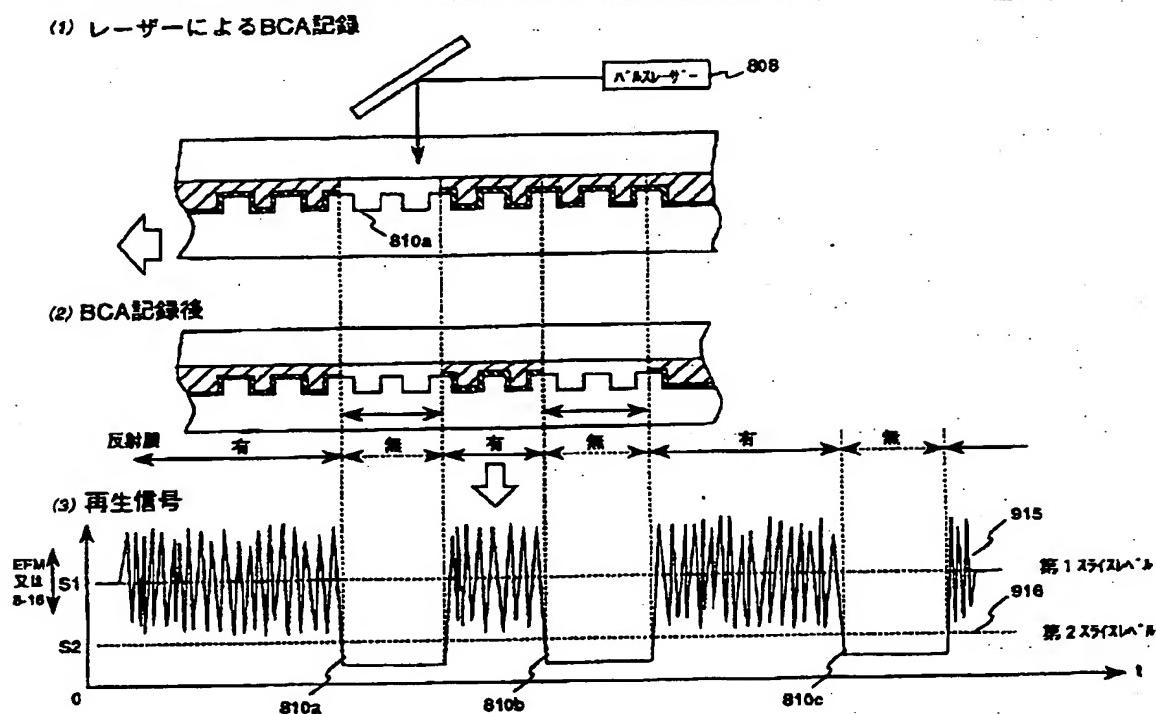


圖一

WO 97/14144

2/27

## 第2図

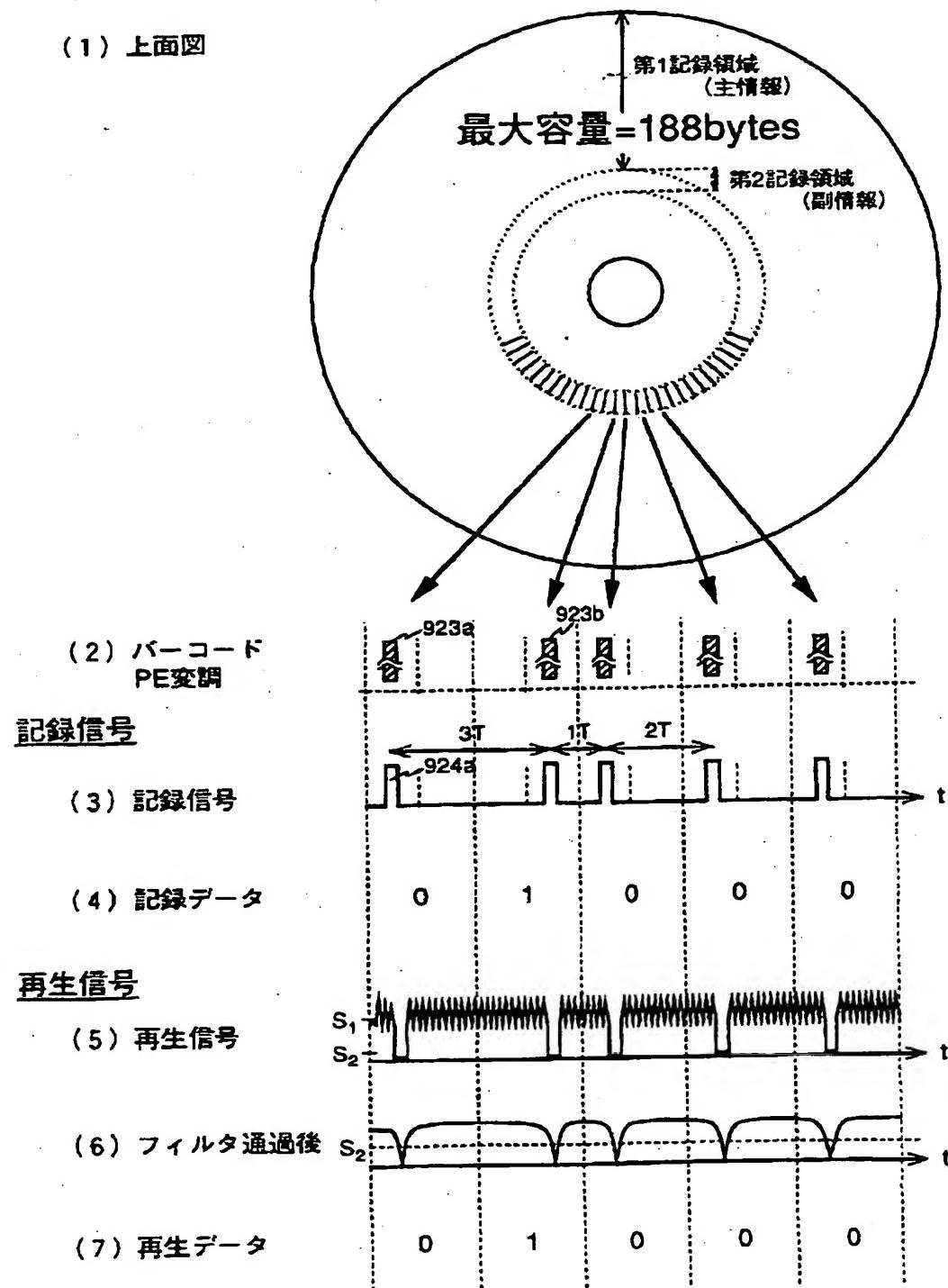


WO 97/14144

PCT/JP96/02924

3/27

## 第3図

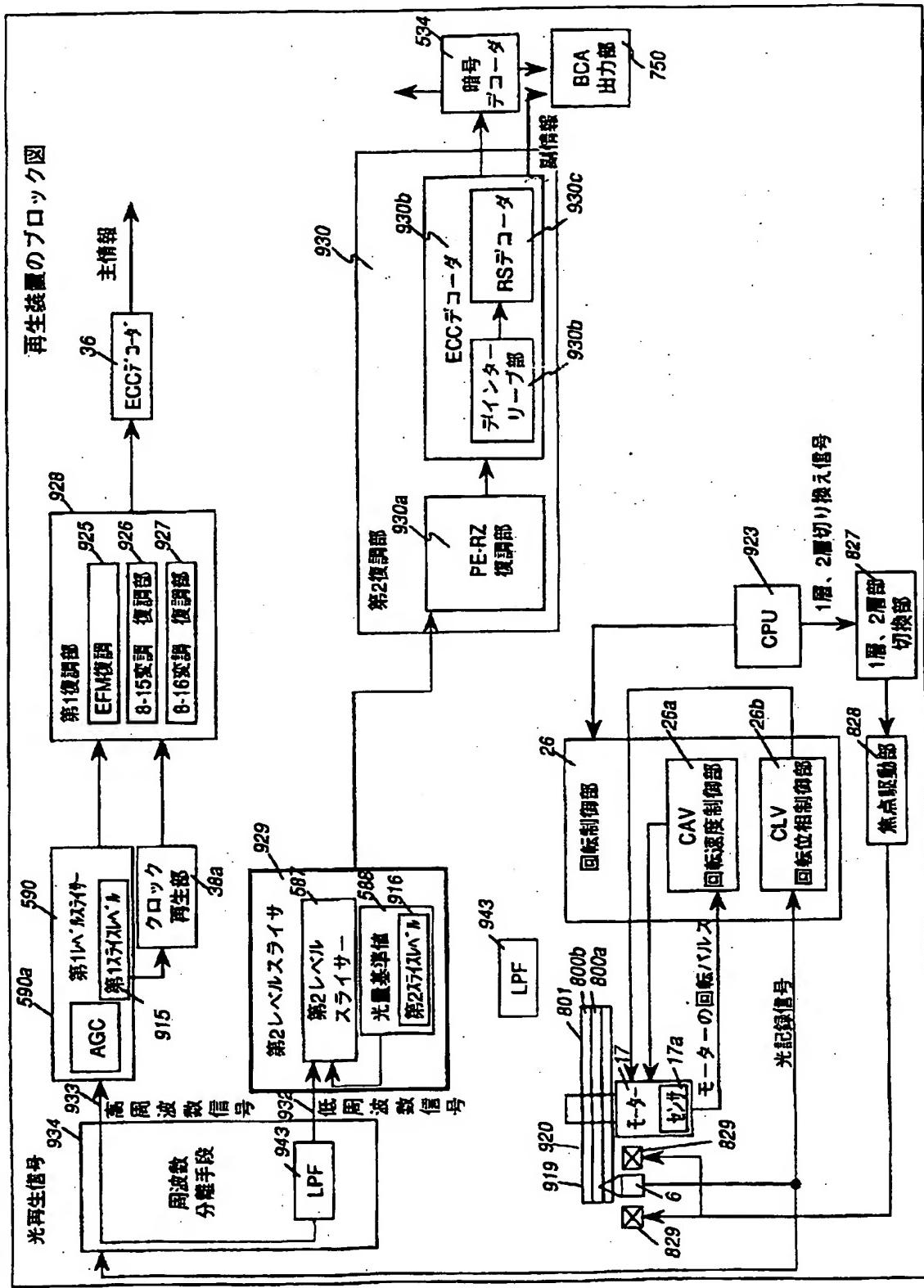


WO 97/14144

PCT/JP96/02924

4/27

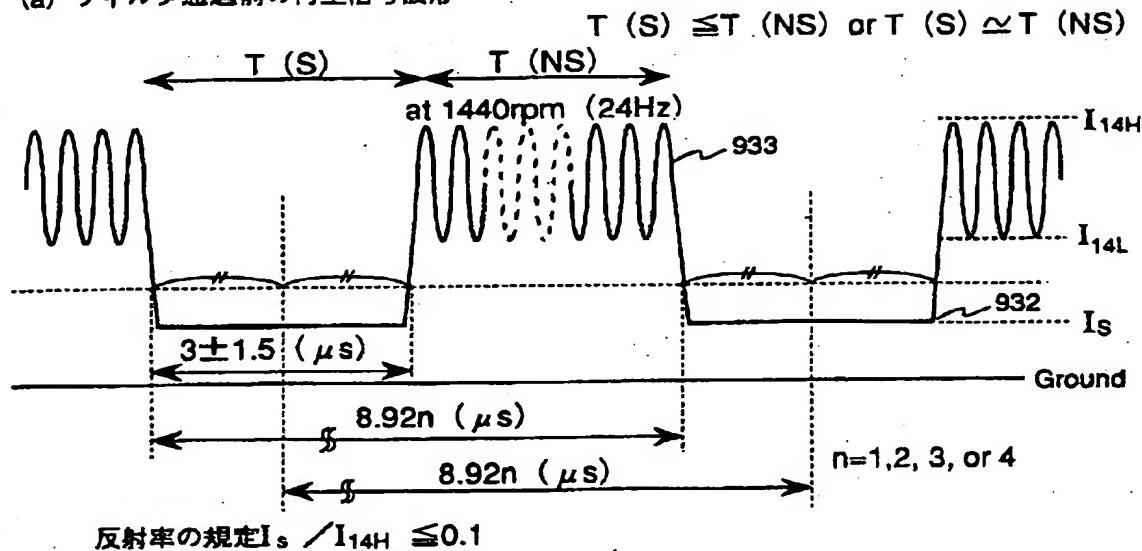
第4図  
再生装置のブロック図



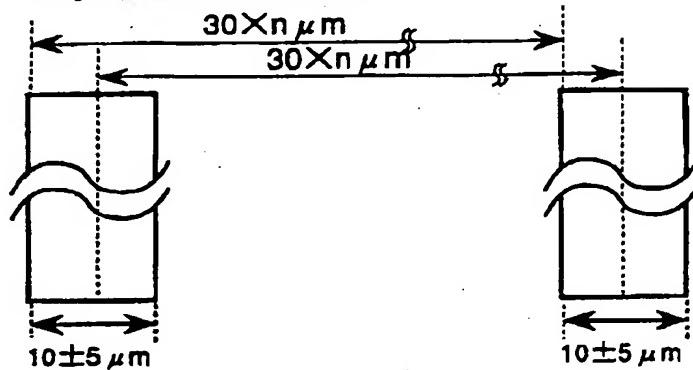
5/27

## 第5図

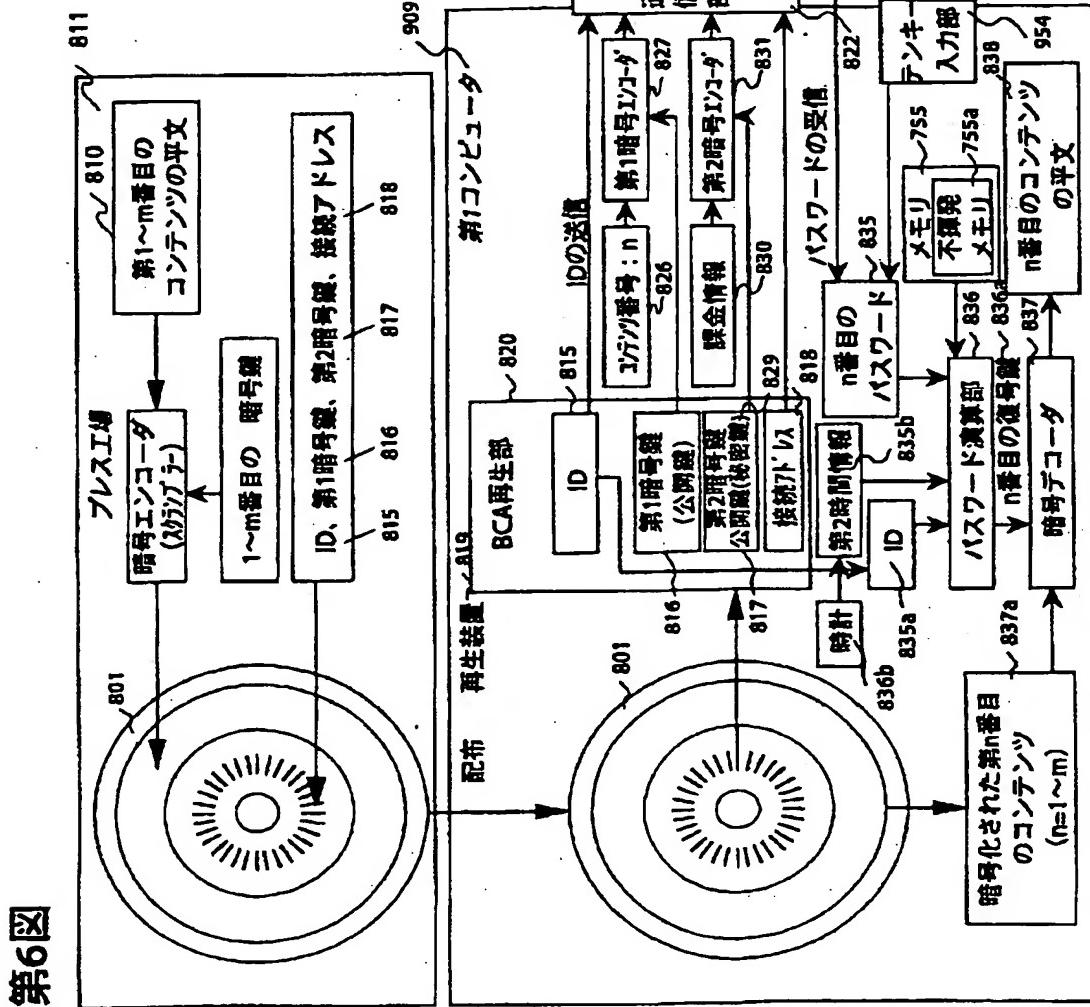
(a) フィルタ通過前の再生信号波形



(b) スリットの寸法精度 (at r=22.2mm)



6/27

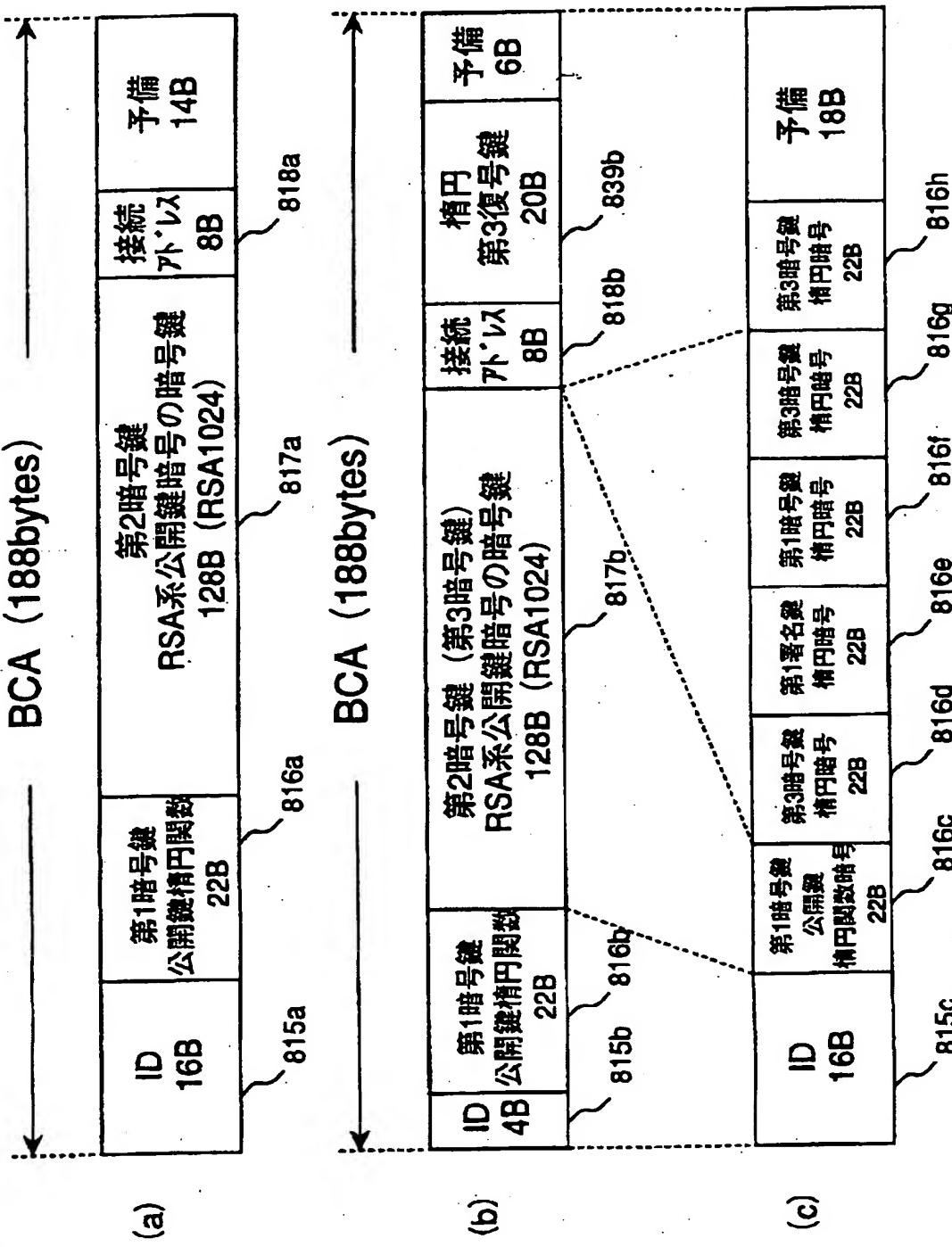


WO 97/14144

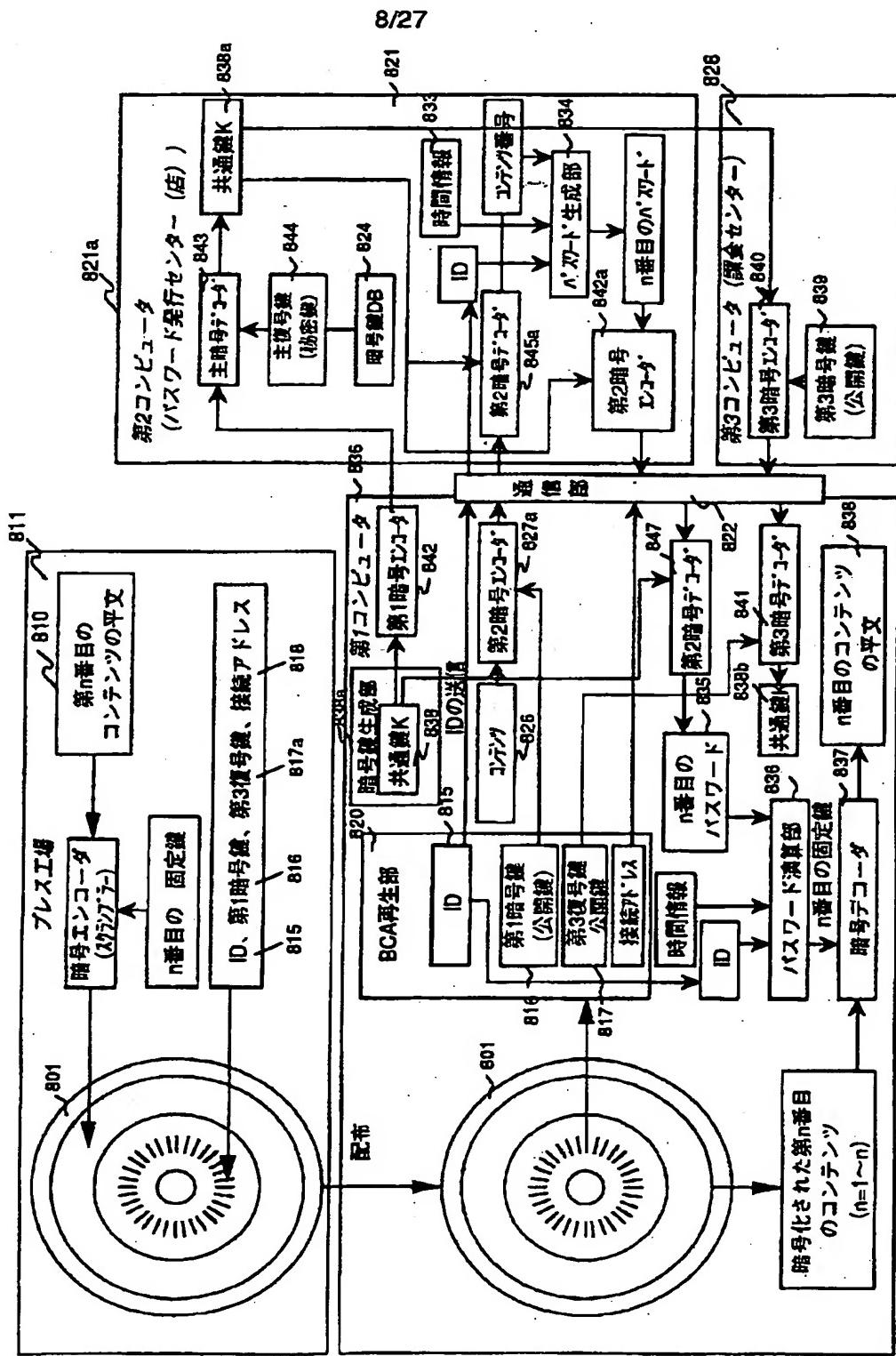
PCT/JP96/02924

7/27

第7図  
BCA (188bytes)



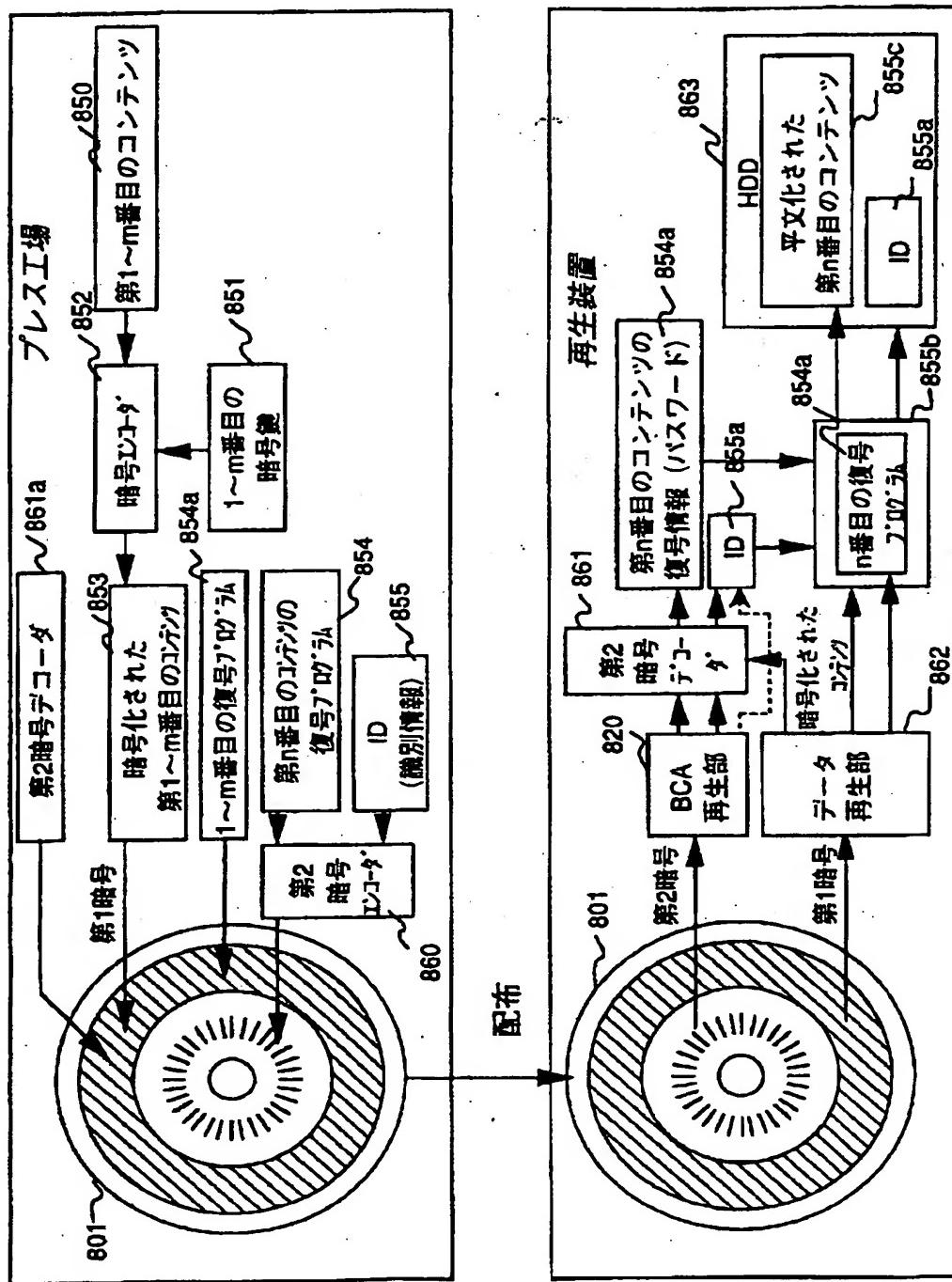
第8図



WO 97/14144

PCT/JP96/02924

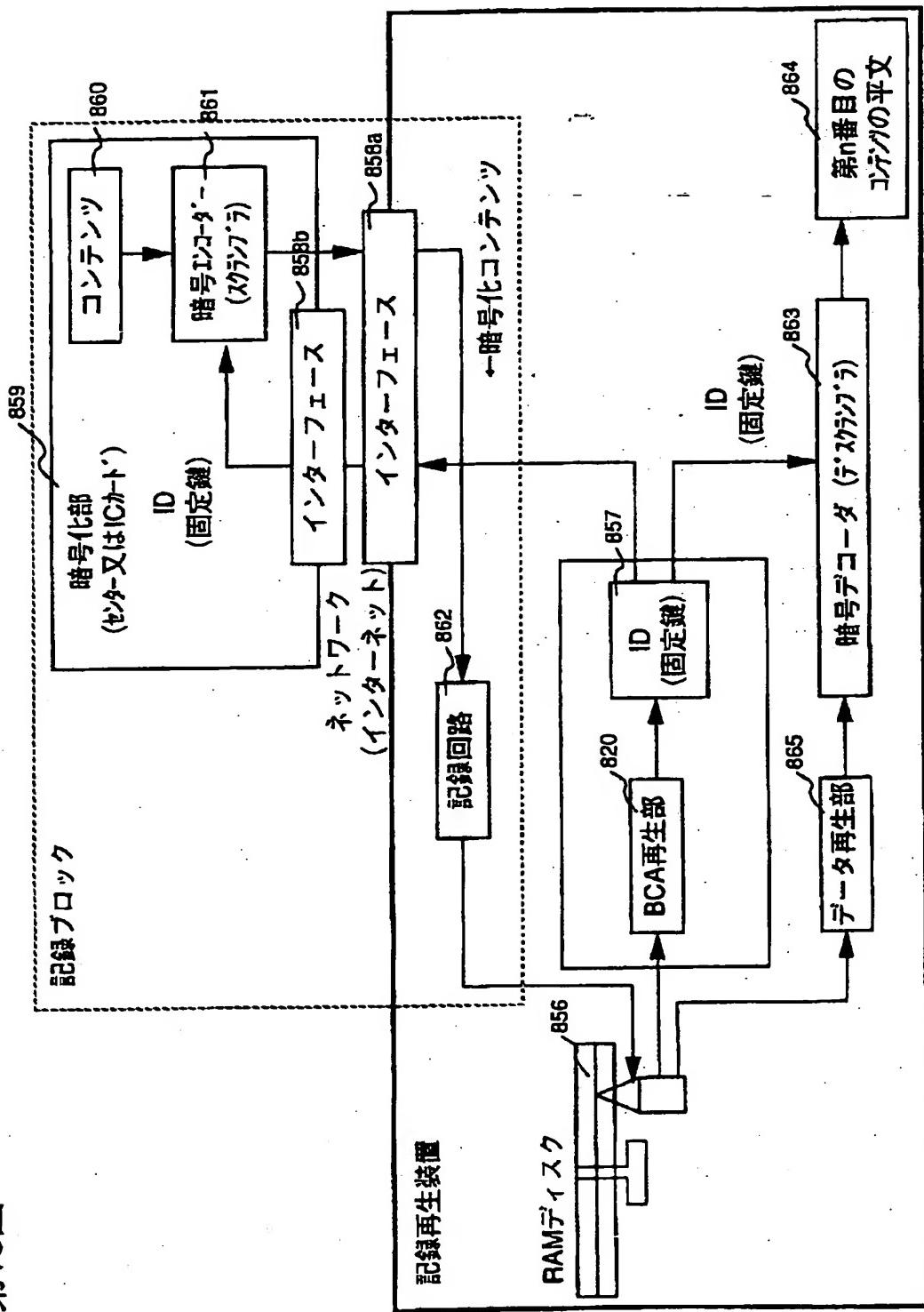
9/27



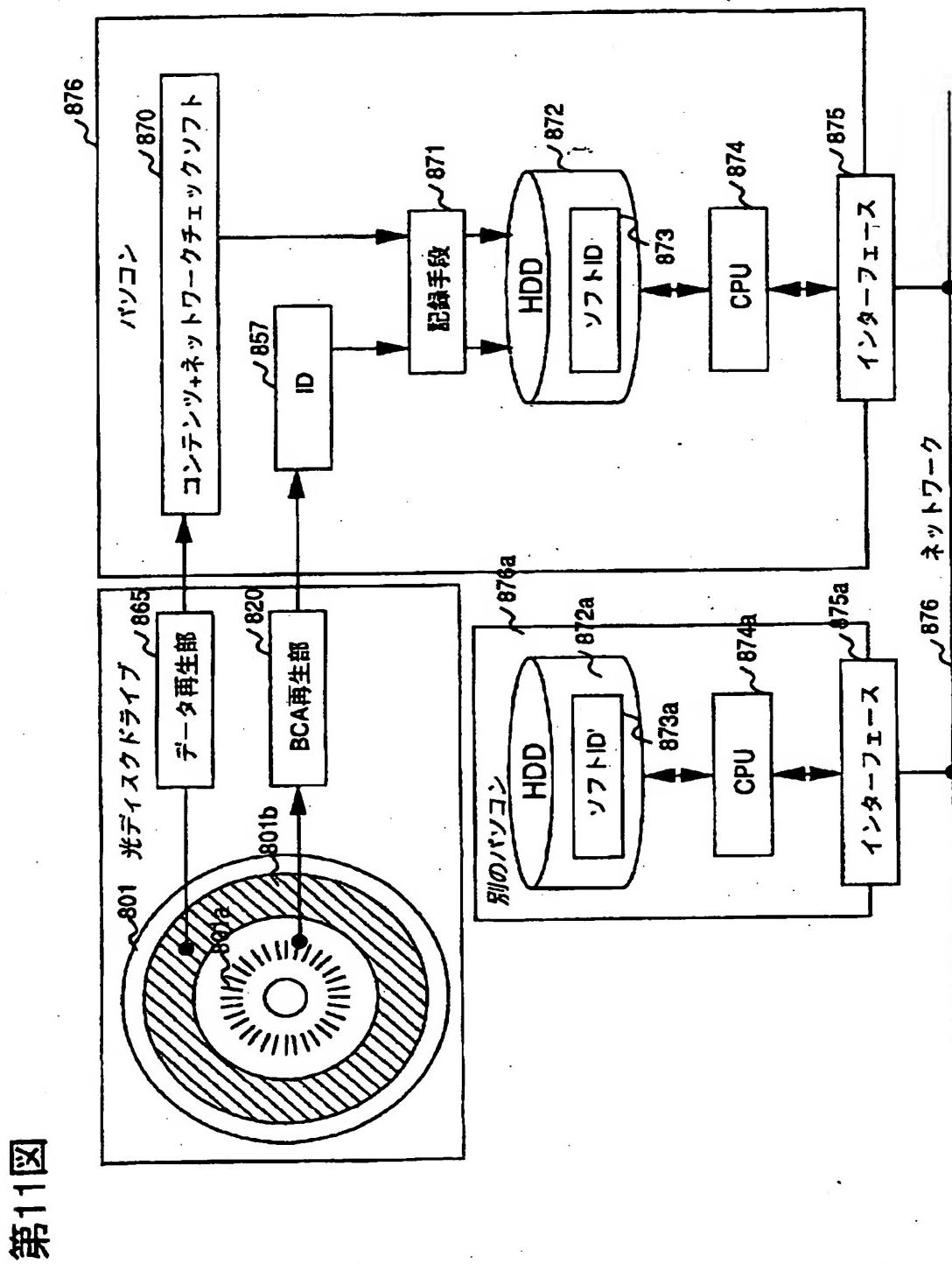
第9圖

10/27

第10図



11/27

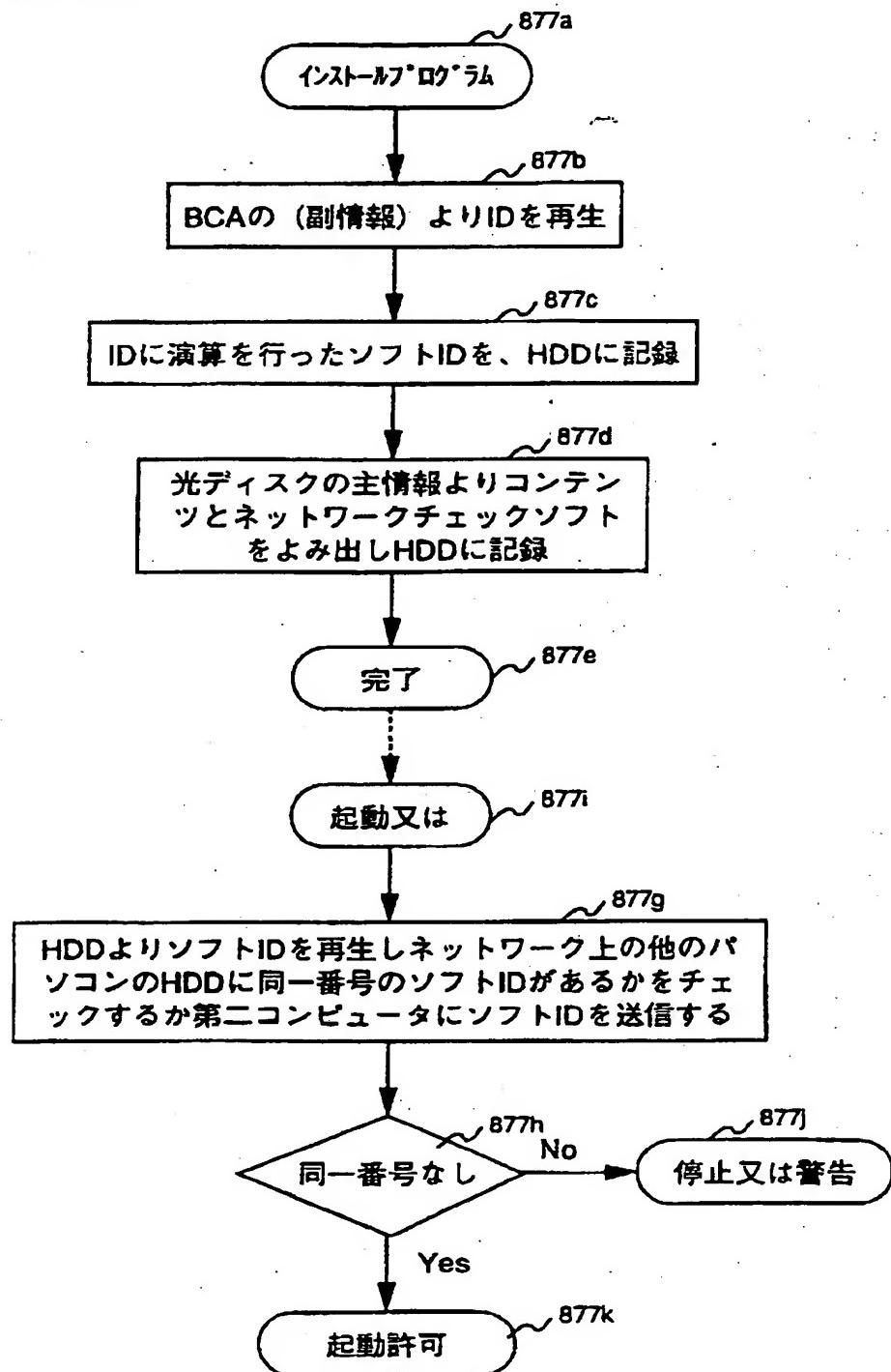


WO 97/14144

PCT/JP96/02924

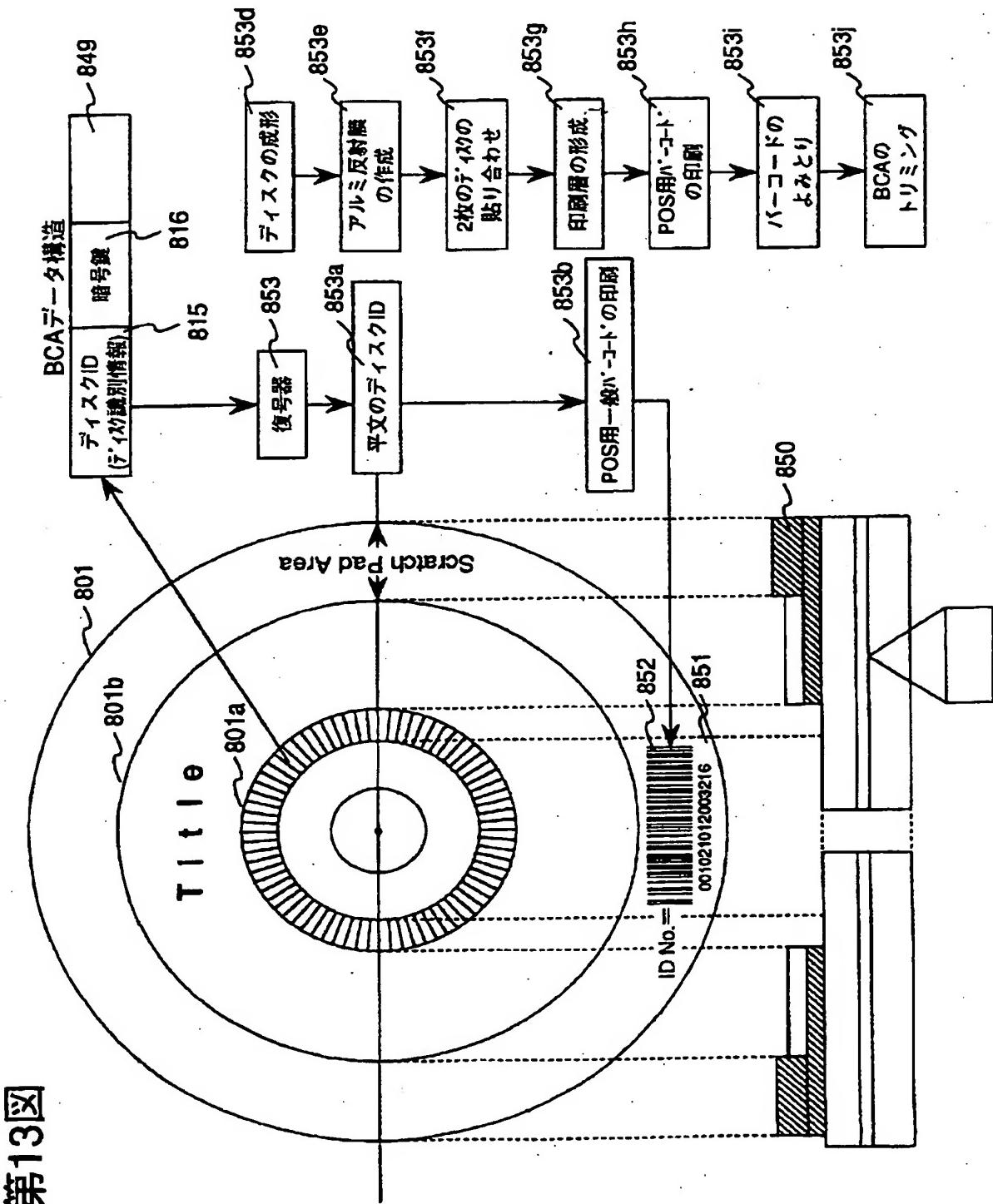
12/27

## 第12図



WO 97/14144

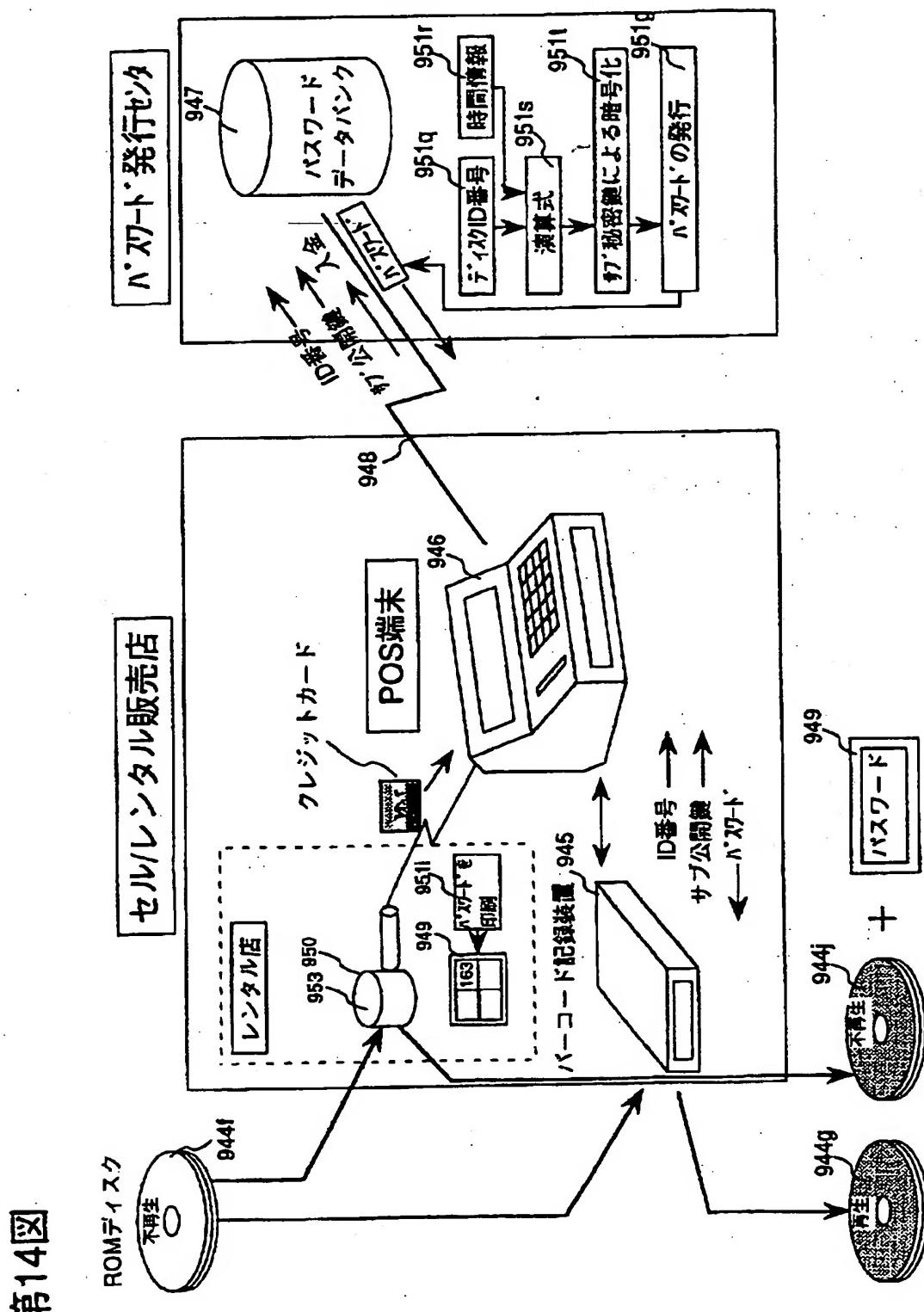
13/27



第13図

WO 97/14144

14/27

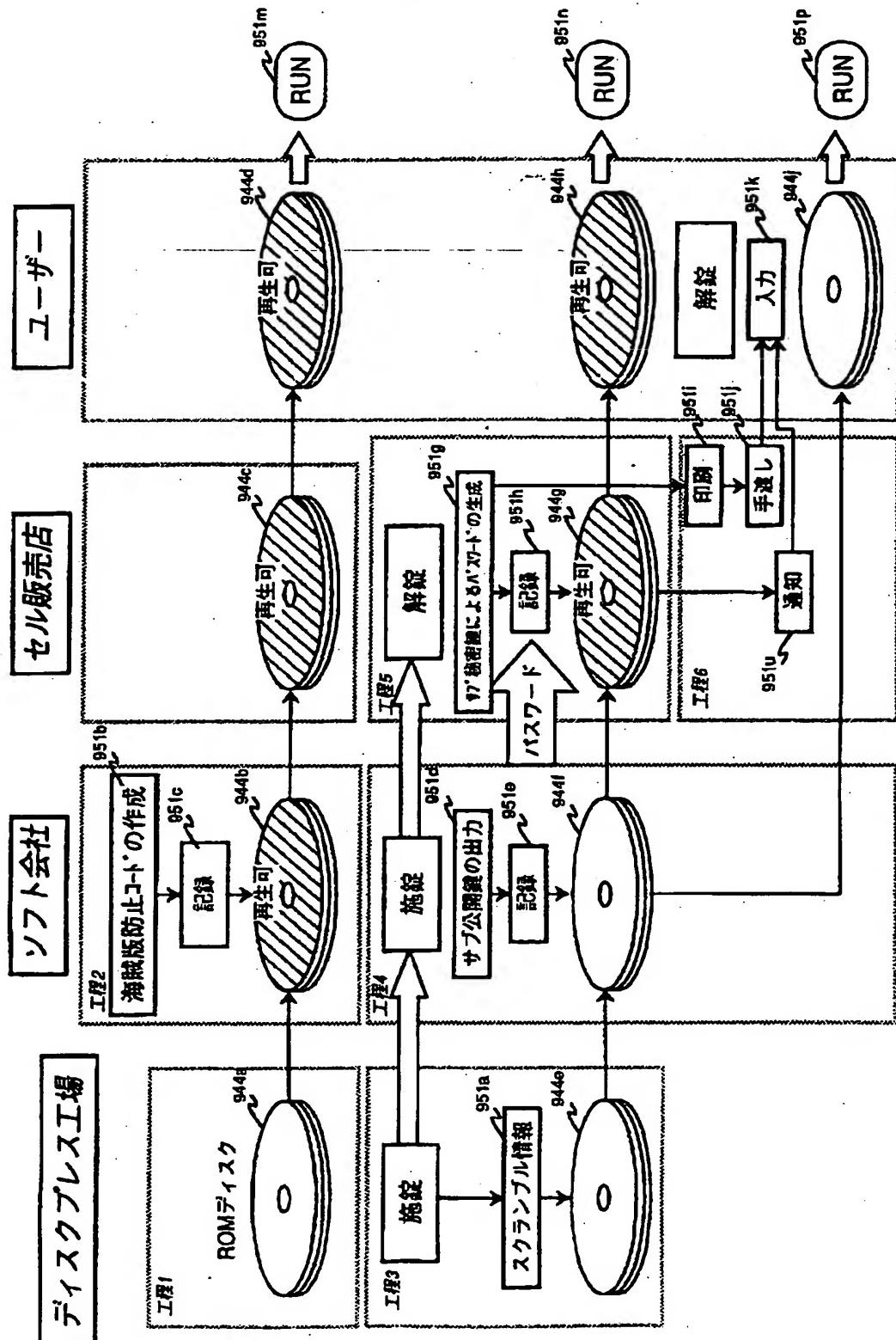


WO 97/14144

PCT/JP96/02924

15/27

第15圖



WO 97/14144

16/27

## 第16図

## 暗号データの復号方法

865

## 暗号データと個別IDのユーザーへの配布

865a

1枚の原盤のROM領域に秘密の第1暗号鍵で暗号化されたmヶのデータと暗号化されたmヶのデータの復号プログラムを記録

865b

原盤より基板を成形し、2枚の基板を貼り合わせてROMディスクを複数枚作成

865c

完成ディスクの書換できない副記録領域(BCA)に、暗号化データの復号に必要な復号情報(プレスしたディスク毎に異なるディスク識別情報 and/or 暗号データの復号鍵)をROM領域と異なる変調方法で記録

865d

ユーザーはディスクを再生し、暗号化データnを選択

865e

ユーザーの情報処理装置で、ROM領域から暗号化データと復号プログラムを再生し、副記録領域から、復号情報を読み出す。

No

オンラインで第2復号情報を得る?

865f

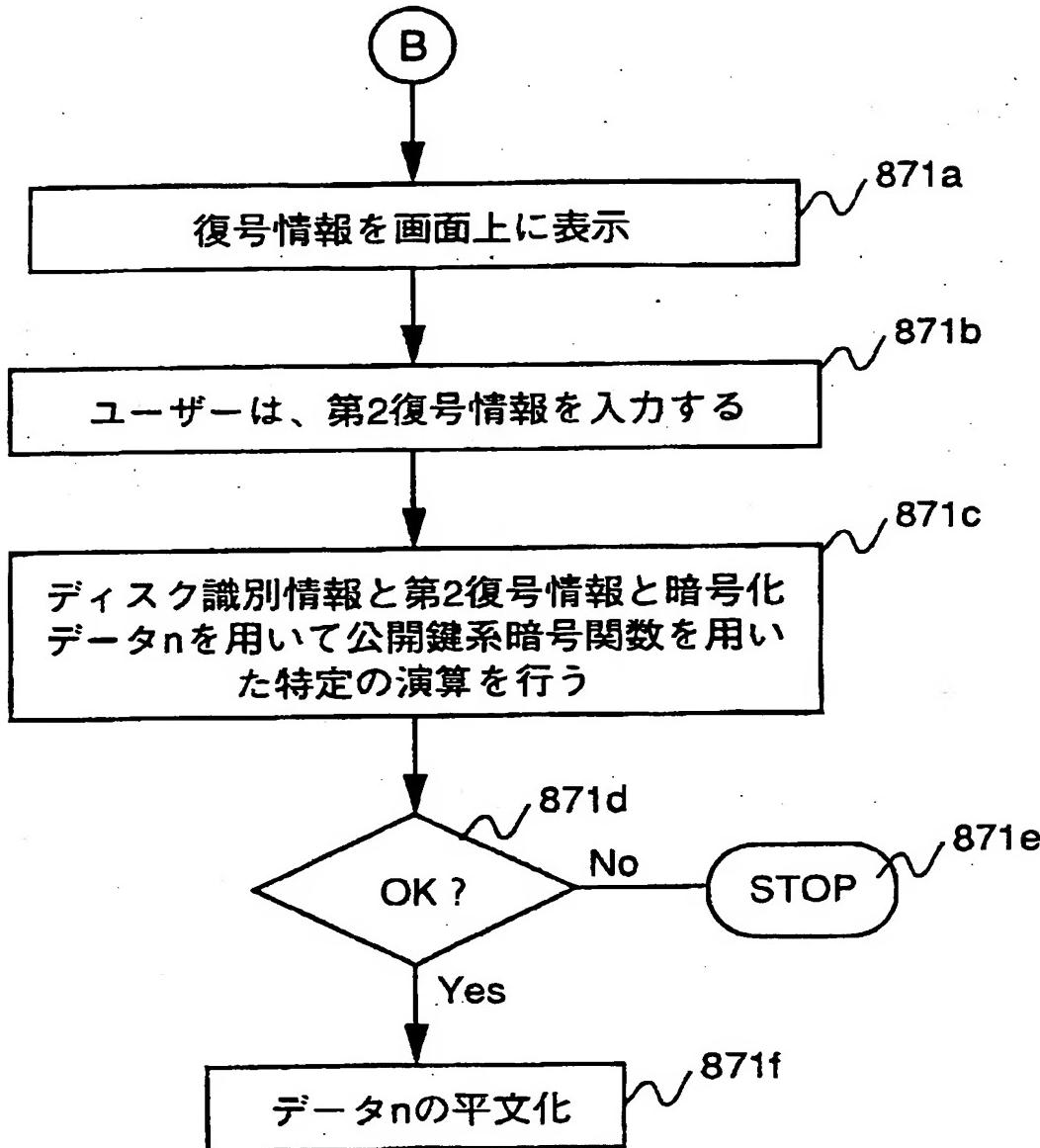
Yes

B

A

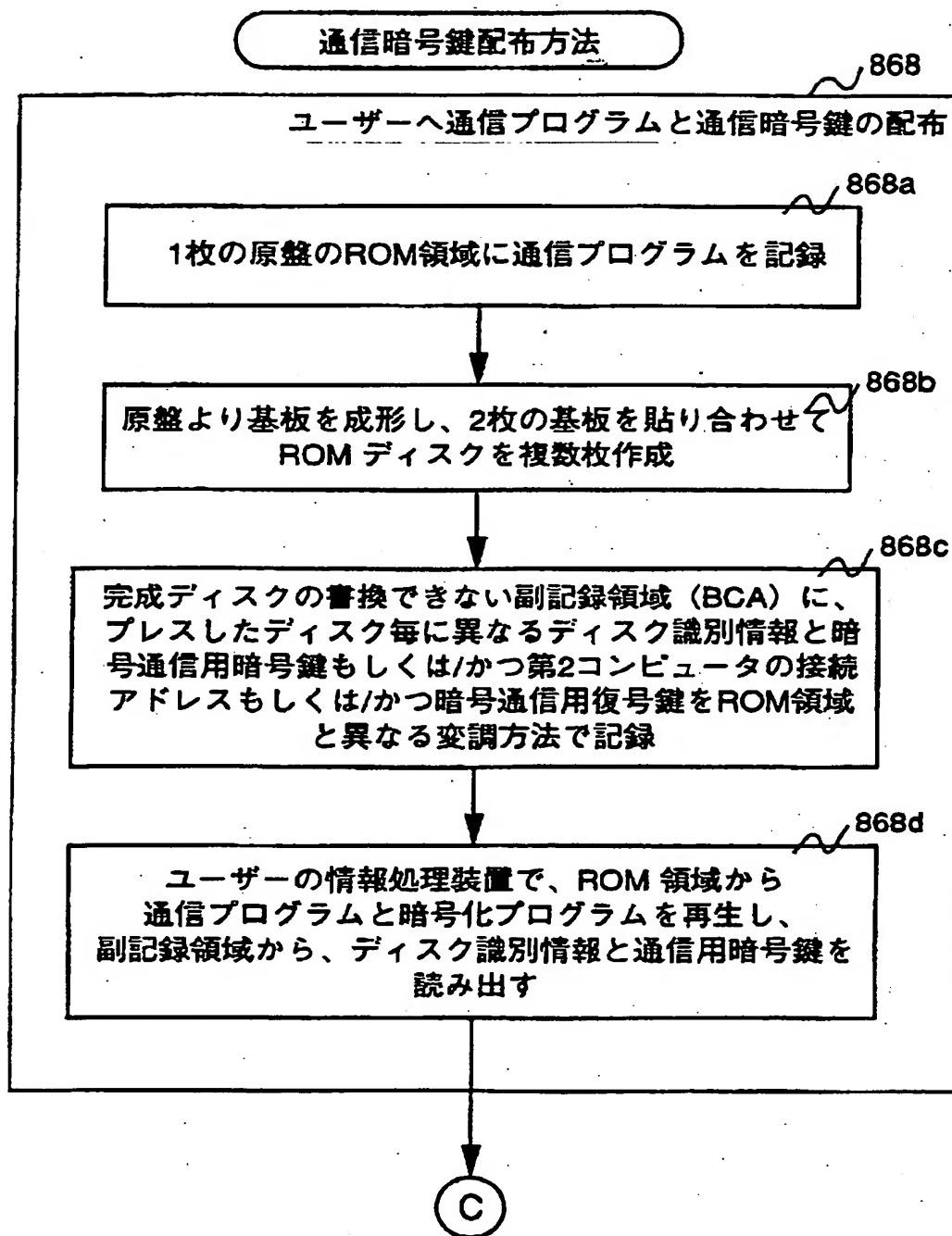
17/27

## 第17図



18/27

## 第18図

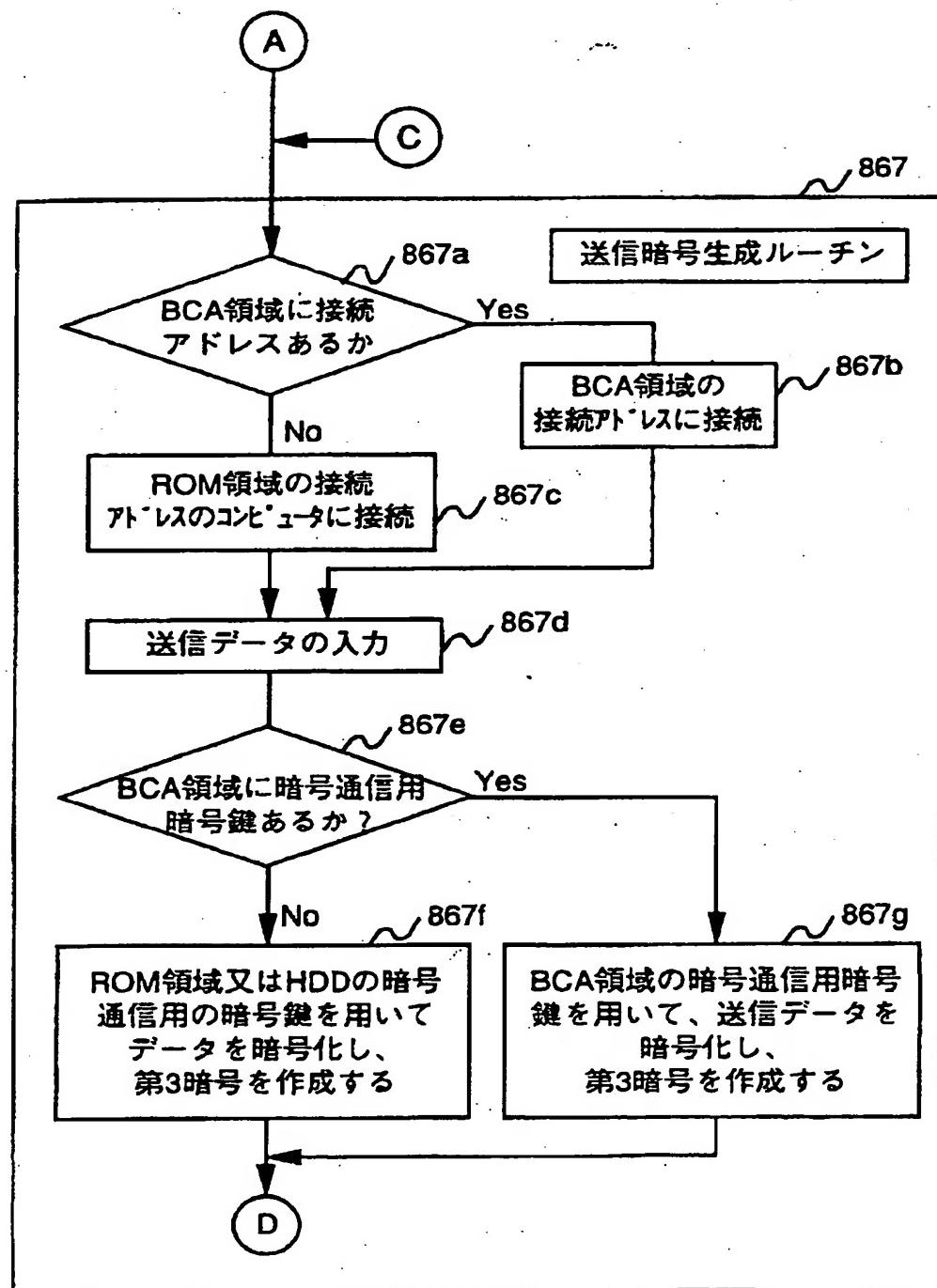


WO 97/14144

PCT/JP96/02924

19/27

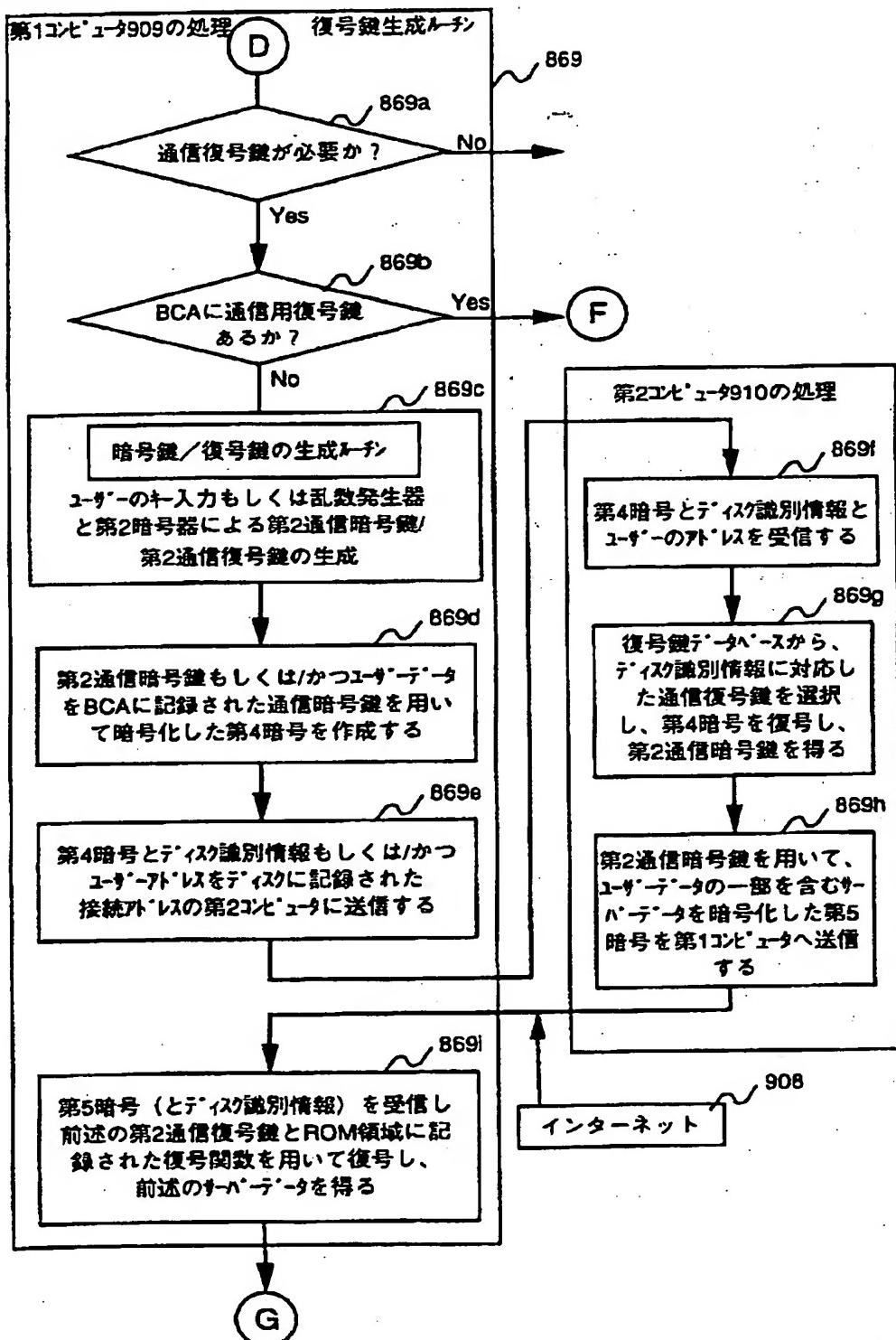
## 第19図



WO 97/14144

20/27

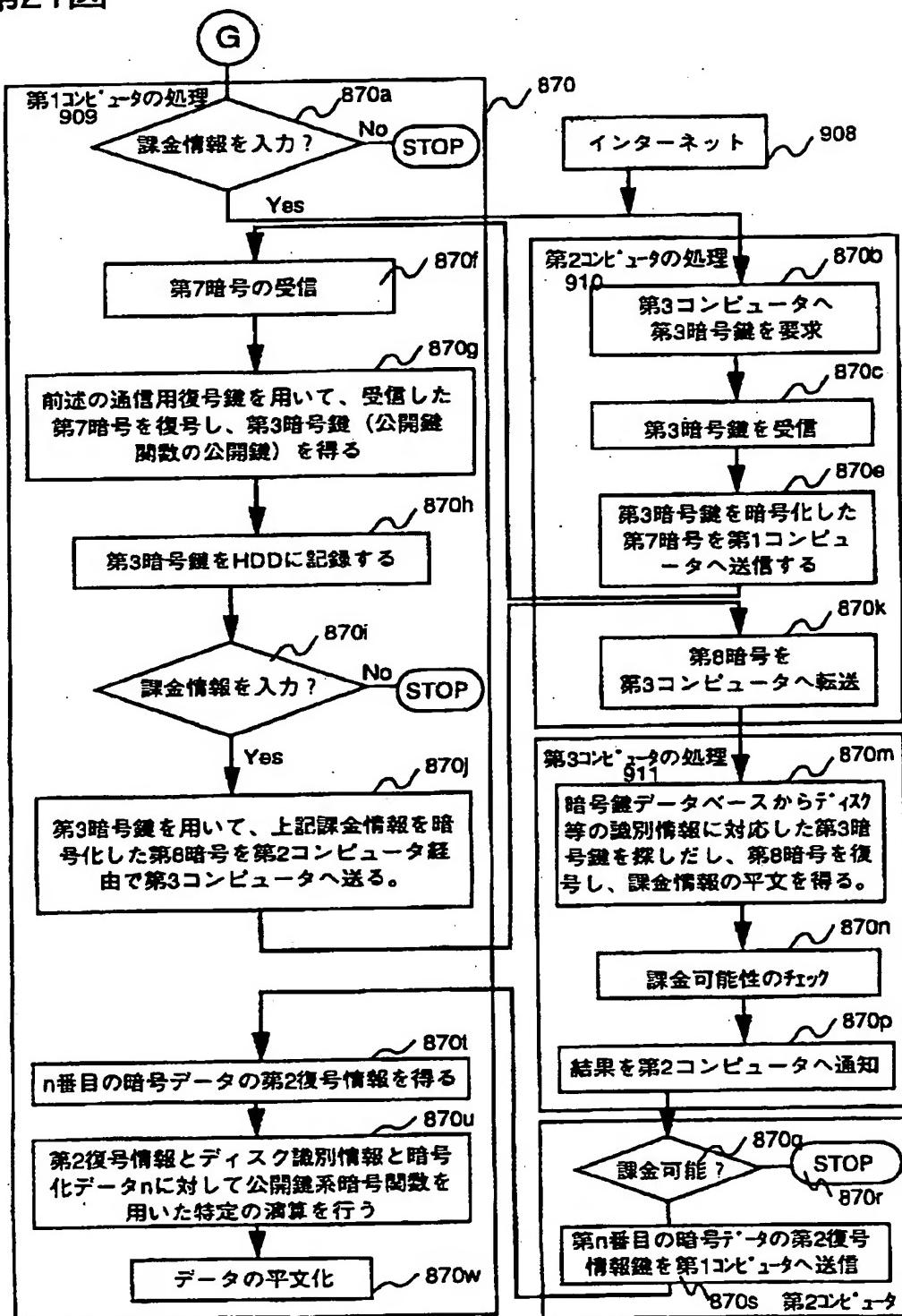
## 第20図



WO 97/14144

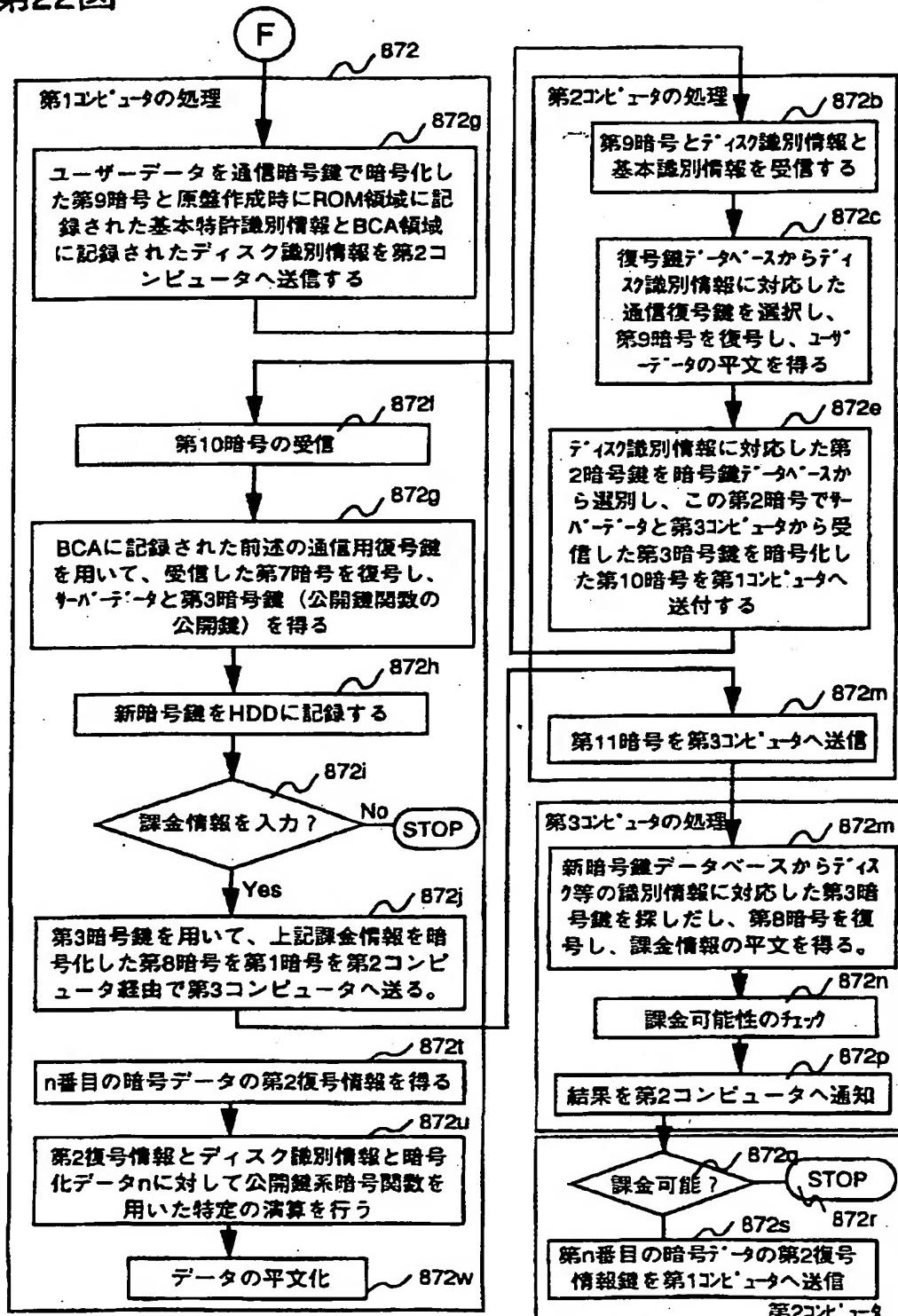
21/27

## 第21図



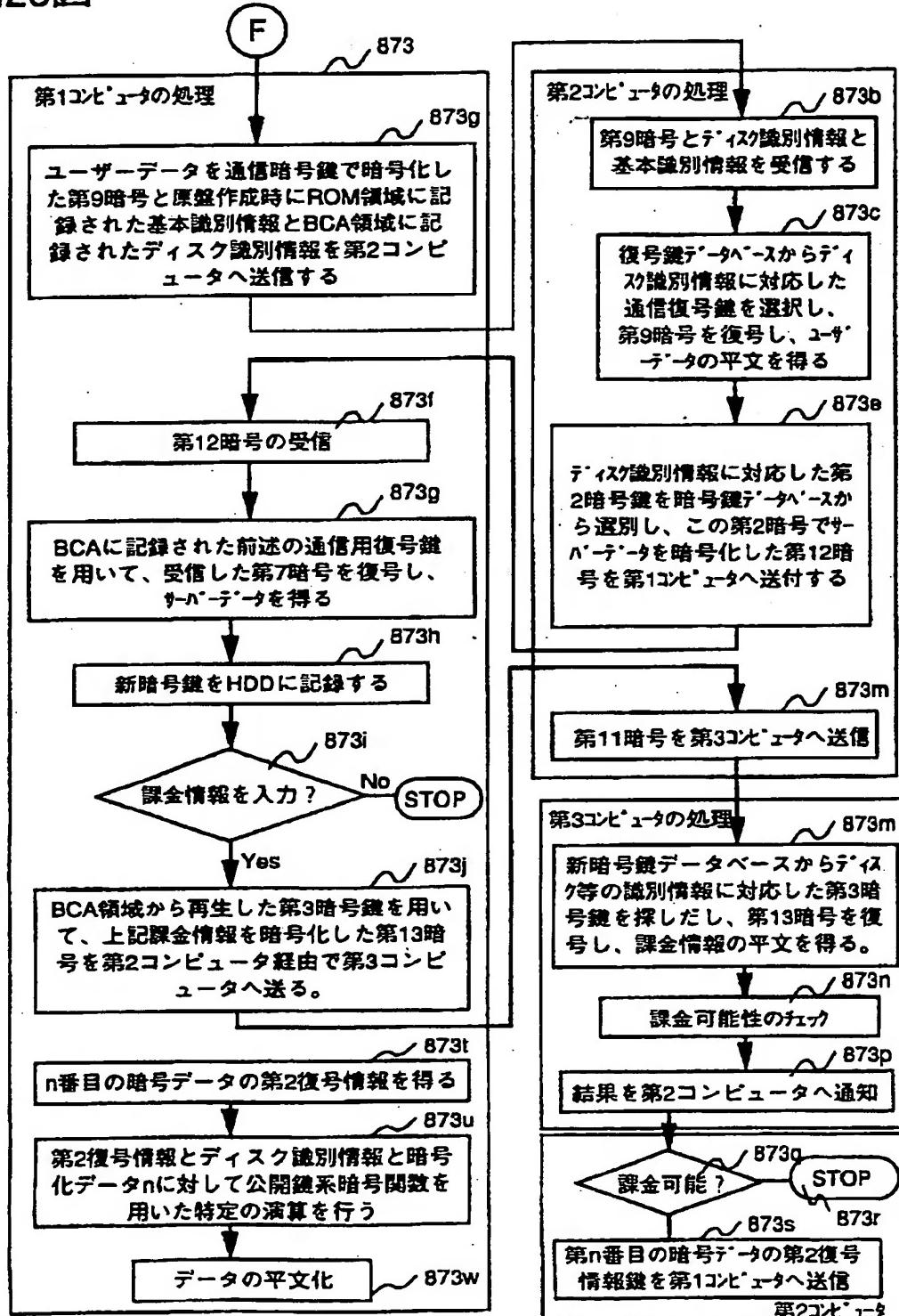
22/27

## 第22図



23/27

## 第23図

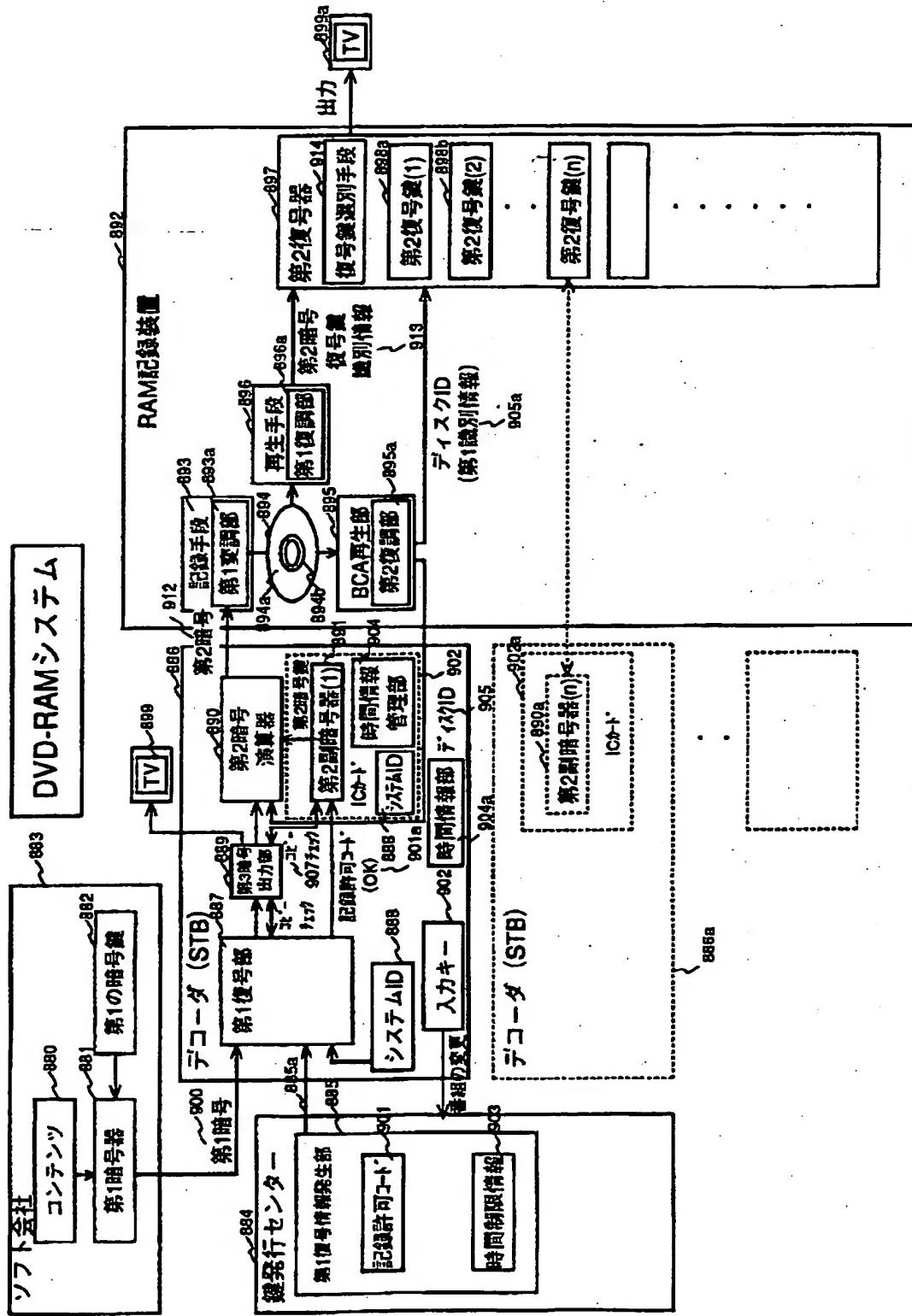


WO 97/14144

PCT/JP96/02924

24/27

第24図



WO 97/14144

PCT/JP96/02924

25/27

## 図面の参考符号の一覧表

- 801… BCA付ディスク  
802… 固定鍵  
803… 暗号エンコーダ  
804… 記録手段  
805… コンテンツ  
806… ID  
807… トリミング装置  
808a… 成形機  
808b… 反射膜作成機  
808c… 貼り合わせ機  
809… 完成ディスク  
809a… 片面ディスク  
809b… 片面ディスク  
811… プレス場  
813… 固定鍵  
814… BCA領域  
815… ディスクID  
816… 第1暗号鍵（秘密鍵）  
817… 第2暗号鍵（秘密鍵）  
818… 接続アドレス  
819… 再生装置  
820… BCA再生部  
821… パスワード発行センター  
822… 通信部  
823… ネットワーク  
824… 暗号鍵DB  
825… 第1復号鍵  
826… コンテンツ番号

WO 97/14144

26/27

- 827… 第1暗号デコーダ  
828… 課金センター  
829… 第2復号鍵  
830… 課金情報  
831… 第2暗号エンコーダ  
832… 第2暗号デコーダ  
833… 時間情報  
834… パスワード生成部  
835… パスワード  
836… パソコン  
837… 第3復号鍵  
838… 共通鍵  
839… 第3暗号鍵  
840… 第3暗号エンコーダ  
841… 第3暗号デコーダ  
842… 主暗号エンコーダ  
843… 主暗号デコーダ  
844… 主復号鍵  
845… 第1暗号デコーダ  
846… 暗号エンコーダ  
847… 暗号デコーダ  
849… BCAデータ  
850… 書き込み層  
851… 文字  
852… 一般バーコード  
853… 復号器  
860… 第2暗号エンコーダ  
861… 第2暗号デコーダ  
862… データ再生部

WO 97/14144

PCT/JP96/02924

27/27

- 863… ROM領域  
864… 追記領域  
865… 復号のフローチャート  
890… 第2暗号演算器  
894a… 第1記録領域  
908… インターネット  
909… 第1コンピュータ  
910… 第2コンピュータ  
911… 第3コンピュータ  
912… 第2暗号  
913… 復号鍵識別情報  
914… 復号鍵選別手段  
915… 第1スライスレベル  
916… 第2スライスレベル  
917… PE-RZ変調器  
918… 透明基板  
919… 第1記録領域  
920… 第2記録領域  
921… ディスクID  
922… BCAフラグ  
923… CPU  
924… コントロールデータ  
925… EFM復調  
926… 8-15変調復調  
927… 8-16変調復調  
928… 第1復調部  
930… 第2復調部  
931… 接続アドレス

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP96/02924

## A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl<sup>6</sup> G11B7/00, G11B20/10, G06F12/14, G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl<sup>6</sup> G11B7/00, G11B20/10, G06F12/14, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1955 - 1996

Kokai Jitsuyo Shinan Koho 1971 - 1996

Toroku Jitsuyo Shinan Koho 1994 - 1996

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 58-21143, A (Sony Corp.), December 8, 1983 (08. 12. 83) (Family: none)	1 - 28
A	JP, 61-71487, A (Hoya Corp.), April 12, 1986 (12. 04. 86) (Family: none)	1 - 28
A	JP, 2-293930, A (Victor Co. of Japan, Ltd.), December 5, 1990 (05. 12. 90) & US, 5379433, A	1 - 28
A	SHINGAKU GIHO Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, September 21, 1994 Makoto Yoshioka, Ryota Akiyama "Trend of Superdistribution Technology" pp. 67-74	6 - 28
A	SHINGAKU GIHO Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, September 21, 1994	6 - 28

 Further documents are listed in the continuation of Box C. See patent family annex.

## \* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed
- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "Z" document member of the same patent family

Date of the actual completion of the international search

December 5, 1996 (05. 12. 96)

Date of mailing of the international search report

December 17, 1996 (17. 12. 96)

Name and mailing address of the ISA/

Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP96/02924

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
-	Yoshimichi Nakazawa "Software Distribution Technology with CD-ROM" p. 41-46	

## 国際調査報告

国際出願番号 PCT/JP96/02924

## A. 発明の属する分野の分類(国際特許分類(IPC))

Int. C1  
G11B 7/00 G11B20/10 G06F12/14 G06F 9/06

## B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. C1  
G11B 7/00 G11B20/10 G06F12/14 G06F 9/06

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1955-1996年

日本国公開実用新案公報 1971-1996年

日本国登録実用新案公報 1994-1996年

## 国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 58-21143, A (ソニー株式会社) B. 12月. 1983 (08. 12 . 83) (ファミリーなし)	1-28
A	JP, 61-71487, A (ホーヤ株式会社) 12. 4月. 1986 (12. 04 . 86) (ファミリーなし)	1-28
A	JP, 2-293930, A (日本ピクター株式会社) 5. 12月. 1990 (05 . 12. 90) & US, 5379433, A	1-28
A	信学技報 Vol. 94, No. 240, 電子情報通信学会技術研究報告, 情報セキュリティ, I SEC 94-13~22, 21. 9月. 1994 吉岡誠, 秋山良太 「超流通技術動向」 p 67-74	6-28

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」先行文献ではあるが、国際出願日以後に公表されたもの

「L」優先権主要に意義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

## 国際調査を完了した日

05. 12. 96

## 国際調査報告の発送日

17.12.96

## 国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100

東京都千代田区霞が関三丁目4番3号

## 特許庁審査官(権限のある職員)

中野 浩昌

5D 9464

電話番号 03-3581-1101 内線 3553

## 国際調査報告

国際出願番号 PCT/JP96/02924

C(続き) .	関連すると認められる文献	関連する 請求の範囲の番号
A	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 信学技術 Vol. 94, No. 240, 電子情報通信学会技術研究報告. 情報セキュリティ, ISEC94-13~22, 21, 9月, 1994 中澤良充 「CDROMによるソフトウェア流通技術」 p 41-46	6-28

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**